The Safety-Critical Systems Club Newsletter

Safety Systems

Vol 31 No. 3 – Oct 2023

STANDARD GAUGE

Recent developments in railway standards



IT'S A ZOO OUT THERE!

Developments in categorising data risk

ENCHANTRESS OF NUMBERS

Reflections on Ada Lovelace Day

For everyone working in Systems Safety

SCSC

thescsc.org



SCSC Publication Number: SCSC-185

While the authors and the publishers have used reasonable endeavours to ensure that the information and guidance given in this work is correct, all parties must rely on their own skill and judgement when making use of this work and obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this work. Neither the authors nor the publishers make any representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to such information and guidance for any purpose, and they will not be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever (including as a result of negligence) arising out of, or in connection with, the use of this work. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of their employers, the SCSC or other organisations.

© SCSC CIC 2023 except where explicitly stated for specific articles, reports or images.

Front cover: Photo 47917112 © Peerajit Ditta In | Dreamstime.com
In Brief images on page 4 may be subject to copyright – see scsc.uk/f138 for details.

Contents

WELCOME

Editorial 3

Opening words from the SCSC Newsletter Editor.

In Brief 4

Recent system safety news items from around the world.

FEATURES

Reflections on Ada Lovelace Day 5

Wendy Owen showcases Ada Lovelace Day and provides further stories from some of the woman of the SCSC.

Software in Railway Applications 13

Lucia Capogna discusses current railways standards and recent developments in their evolution.

The Data Risk Zoo 21

Mike Parsons and Paul Hampton provide an update on further developments in the categorisation of data safety risk.

How Do I Get Into Safety? 33

More insights on how safety careers started from the SCSC Steering Group.

REPORTS

National Space Centre Tech Trip Report 37

Mike Parsons reports from the last SCSC Tech Trip.

Book Review 44

Somnath Pal reviews Gill Kernick's book "Catastrophe and Systemic Change".

60 Secs with ... Davy Pissoort 46

Davy answers some quick-fire questions on system safety and life!

Recent Publications 43

Recent system-safety related publications.

GROUPS

Working Groups 51

Details of the SCSC Working Groups.

SCSC Steering Group 57

Who's who in the Steering Group.

EVENTS

Calendar 59

Events Diary 60

THE SAFETY-CRITICAL SYSTEMS CLUB

Safety-Critical Systems Symposium (SSS'24)

The programme encompasses three days of presentations including keynote talks, submitted papers, posters, interactive sessions, updates from the SCSC Working Groups, and a vendor exhibition.

Seven eminent speakers have kindly agreed to give keynote talks and Simon Davies will give the after-dinner talk on the Wednesday evening.

Symposium Website: scsc.uk/sss

Keynote Speakers

The Keynote speakers are: Adiac Aguilar, Volvo Cars; Mikela Chatzimichailidou, University College London; Dewi Daniels, Software Safety Ltd, Simon Davies, Vertical Aerospace Group Ltd; Phil Koopman, CMU; Alessio Lomuscio, Imperial College and Hayat Zerkani, Crossrail Ltd.

Adiac Aguilar, Autonomous Systems and Safety | Core System Platform Architecture at Volvo Cars.

Mikela Chatzimichailidou, Professor in Design for Mobility, Health, People and Society, University College London.

Dewi Daniels, Software Safety Ltd.

Simon Davies, Test Pilot, Vertical Aerospace Group Ltd.

Phil Koopman, Associate Professor, Carnegie Mellon University (CMU)

Alessio Lomuscio, Professor of Safe Artificial Intelligence at Imperial College London. Founder and CEO at Safe Intelligence**.**

Hayat Zerkani, Head of System Safety and Interoperability at Crossrail Ltd.

Panel Speakers

The Safe AI panel speakers are:

- **Phil Koopman**, CMU;
- **Alessio Lomuscio**, Imperial College London and Safe Intelligence
- **John McDermid**, Assuring Autonomy International Programme
- **Helen Monkhouse**, HORIBA MIRA
- **Mark Sujan**, Health Services Safety Investigation Body (HSSIB)

Editorial



Tuesday 10th October 2023 marks "Ada Lovelace Day" – an international day celebrating the achievements of women in science, technology, engineering and maths.

Ada appeared on the front cover of the May 2023 edition of the newsletter as our lead article was from Wendy Owen celebrating the woman of the SCSC and coinciding with International Women in Engineering Day (23rd June 2023).

In this edition Wendy Owen expands on her earlier article by exploring who Ada was, her background and her remarkable achievements as well as talking to a few of our modern-day "Adas"!

In our second article, Lucia Capogna discusses current railways standards and recent developments in their evolution. As well as providing background for those unfamiliar with the standards, she provides insights through interviews with two members of the CENELEC working group on their thoughts about the new software standard and the future of software.

Our third article covers some developments in the area of data safety risk categorisation that I have been working on with Mike Parsons. We first introduced these concepts at SSS'23 and now have a taxonomy of terms but it is clear that, not only are there other types of data risk out there, but others are keen to visualise them as animals. You've likely heard of Black Swans no doubt, but what about Grey Swans and Red Swans or even the Boiling Frog! It seems there is a complete zoo out there!

Our "How Do I Get Into Safety?" series returns this month with interesting insights from James Inge and Louise Harney.

Mike Parson's provides a report on the latest Tech Trip to National Space Centre in Leicester with some amazing pictures of the technologies that have taken us into space and beyond.

At SSS'23, Gill Kernick gave, at times, a moving account of her experiences during the events surrounding the Grenfell Tower fire in 2017 and her wider challenges in effecting systemic change. Somnath Pal has very kindly provided a review of her book "Catastrophe and Systemic Change".

I would like to welcome Davy Pissoort as our latest member of the SCSC Steering Group. Davy is Professor at KU Leuven Bruges Campus and I managed to catch up with him for our 60 second interview.

It also gives me great pleasure to see the return of the Safety Systems Crossword! Why not test your knowledge of all matters to do with system safety! There is a prize for the first correct entry drawn out of a hat at SSS'24!

Paul Hampton
SCSC Newsletter Editor
paul.hampton@scsc.uk



In Brief



Beta Technologies Flies Electric Aircraft Across The Border To Canada



Vermont-based electric aircraft developer Beta Technologies flew its Alia prototype into Montréal on Wednesday. With Beta test pilot Chris Caputo at the helm and accompanied by Beta flight test engineer Emma Davis, the Alia prototype took off from the company's flight testing centre in New York and landed about 30 minutes and 64 miles later in Montréal. *futureflight.aero*

Self-driving car systems were involved in 400 crashes since 2021 – 273 were Teslas



Federal regulators found that self-driving AI systems were involved in almost 400 car crashes in the last year, with Teslas accounting for 70 per cent of the accidents.

According to the report, between 1 July of last year and 15 May of this year, there were 392 accidents involving self-driving technologies. In those accidents, six people were killed and five were seriously injured.

Of those 392, Tesla's Autopilot, Full Self Driving mode, or at least a component of its self-driving tech was active in 273 of those crashes. *independent.co.uk*

NATS report into air traffic control incident details root cause

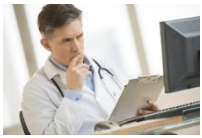


NATS' preliminary investigation has confirmed the root cause that led to air traffic control failures. The report identified an issue with a flight plan processing sub-system called Flight Plan Reception Suite Automated – Replacement (FPRSA-R).

It was found to have encountered an extremely rare set of circumstances presented by a flight plan that included two identically named, but separate waypoint markers outside of UK airspace.

This led to a 'critical exception' whereby both the primary system and its backup entered a fail-safe mode. *nats.aero*

Newcastle Hospitals says computer error lost patient letters



A hospital trust failed to send out 24,000 letters from senior doctors to patients and their GPs after they became lost in a new computer system.

Newcastle Hospitals warned the problem, dating back to 2018, is significant.

The BBC has been told the problems occurred when letters requiring sign-off from a senior doctor were placed into a folder few staff knew existed.
bbc.co.uk

Reflections on Ada Lovelace Day



Watercolour portrait of Ada King, Countess of Lovelace

Following on from her article in the May 2023 edition in the run-up to International Women in Engineering Day (INWED), in this edition, Wendy Owen showcases Ada Lovelace Day – celebrating the achievements of women in science, technology, engineering and maths (STEM) – which this year falls on Tuesday 10th October 2023.

In this article, Wendy describes how Ada is an important part of STEM history, in particular computing, and talks about a few of the modern-day 'Adas' in our midst at SCSC.

Who Was Ada?

Ada was born Ada Gordon in 1815, the sole child of a brief and tempestuous marriage of the erratic poet Lord Byron and his mathematics-loving wife Annabella Milbanke. Fearing that Ada would inherit her father's volatile 'poetic' temperament, her mother raised her under a strict regimen of science, logic and mathematics. As a child, Ada developed a fascination with machines – she designed fanciful boats and steam flying machines, and pored over diagrams of new inventions of the Industrial Revolution that filled the scientific magazines of the time. At 19 she was married to an aristocrat, William King. When he became Earl of Lovelace in 1838 his wife became Lady Ada King, Countess of Lovelace. Hence why she is often called Ada Lovelace, which is a bit incorrect but never mind as it's a fabulous name!

In 1833, Lovelace's mentor (scientist/polymath Mary Sommerville) introduced her to Charles Babbage, a Lucasian Professor of Mathematics. At that time, Babbage had already attained considerable celebrity for his visionary and perpetually unfinished plans for gigantic clockwork calculating machines.

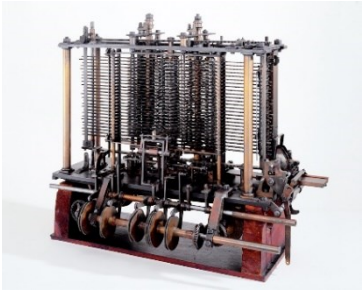
Charles and Ada both had somewhat unconventional personalities and became close and lifelong friends. Babbage described her as:

"*that Enchantress who has thrown her magical spell around the most abstract of Sciences and has grasped it with a force which few masculine intellects could have exerted over it*" and as "*The Enchantress of Numbers".*

How wonderful!

The Analytical Engine

Lovelace was deeply intrigued by Babbage's plans for a tremendously complicated device he called the Analytical Engine, which was to combine the array of adding gears of his earlier Difference Engine with an elaborate punch-card operating system. It was never built, but the design had all the essential elements of a modern computer.



Portion of the calculating machine with a printing mechanism of the analytical engine, built by Charles Babbage, as displayed at the Science Museum (London)

In 1842 Lovelace translated a short article describing the Analytical Engine by the Italian mathematician Luigi Menabrea, for publication in England. Babbage asked her to expand the article "*as she understood the machine so well*". The final article is over three times the length of the original and contains several early 'computer programs,' as well as strikingly prescient observations on the potential uses of the machine, including the manipulation of symbols and creation of music.

Although Babbage and his assistants had sketched out programs for his engine before, Lovelace's are the most elaborate and complete, and were the first to be published; thus, she is often referred to as "the first computer programmer". Babbage himself "*spoke highly of her mathematical powers, and of her peculiar capability — higher than of any one he knew, to prepare the descriptions connected with his calculating machine."*

"The Thrilling Adventures of Lovelace and Babbage: The (Mostly) True Story of the First Computer" [3] provides a wonderfully entertaining insight into Lovelace and Babbage's early exploits.

Thwarted Potential and Legacy

Unfortunately, Ada died of cancer only aged 36, a few short years after the publication of "Sketch of the Analytical Engine, with Notes from the Translator". She lies in the Byron family vault at the Church of St Mary Magdelene in Hucknall, alongside her infamous father.

You can sometimes see Ada's works and personal belongings on display at Newstead Abbey in Nottinghamshire [2]. I went there a few years back during the bicentennial anniversary of her birth and to see such items in person was a truly amazing experience.

In recent decades, Ada's thwarted potential, and her passion and vision for technology, have made her a very powerful symbol for modern women working in technology.



Newstead Abbey in the 1800s

Latest developments in the Ada trail include:

- November 2020, Trinity College (Dublin), whose library had previously held forty busts, all of them men, announced it was commissioning four new busts of women, one of whom was to be Lovelace.
- March 2022, a statue of Ada Lovelace was installed at the site of the former Ergon House in the City of Westminster. The sculpture was unveiled on International Women's Day, 2022.
- September 2022, Nvidia (a gaming/graphics/AI company) announced their Ada Lovelace graphics processing unit (GPU) microarchitecture.
- July 2023, the UK's Royal Mint issued four commemorative £2 coins in various metals to "honour the innovative contributions of computer science visionary Ada Lovelace and her legacy as a female trailblazer."

Turing, Human Computers and ADA

A century on from Ada's life, the Analytical Engine remained a vision until Lovelace's notes became one of the critical documents to inspire Alan Turing's work on the first modern computers in the 1940s, which leads us to where technology is today. We would also see the advent of "human computers" such as those behind the NASA programs of the 1960s as seen in the film Hidden Figures (2016).

We should of course mention ADA, the programming language. This was developed by a French computer scientist Jean Ichbiah of Honeywell under contract to the US DoD between 1977 to 1983, to supersede over 450 other languages in use at the time. It is still named after our Ada, so by the 1970s she was definitely internationally known. I know by the 1980s I was taught about and even used punched cards on some computers.



Anyway, ADA was originally designed for embedded and real-time systems, and is ideal for very large software systems. The way the package specifications and interfaces and runtime checks work enable early problem detection during design phase. It also includes facilities to help Object-Oriented Programming (OOP) and program verification. Hence, ADA is widely used in critical systems, where any anomaly might lead to very serious consequences (accidental death, injury or severe financial loss). Examples of systems where ADA is used include avionics, air traffic control, railways, banking, military and space technology.

In short, ADA has safety-critical support features, is often an integral part of safety-critical systems and we should be very interested in it (alongside derived tools).

Software safety engineering is its own specialised discipline for those who wish to tread the path.

Our Modern 'Adas'

Audrey Canning has over forty years' experience in the application of advanced software control systems, safety-critical computer systems, manufacturing technologies and assurance of major infrastructure projects.



Audrey at the Worshipful Company of Engineers

Her career began as a design engineer developing electronic hardware, firmware and software control and signal processing systems, firstly for Marconi Space and Defence Systems, then for a SME. In 1991 she became a Department Manager at ERA Technology Ltd. During her time at ERA, she was responsible for development of avionics software standards, communication protocols, mine detection radar signal processing algorithms and research into AI.

In 1986 she established ERA's work in safety-critical computer systems (which came to be one of the most highly regarded centres in this field). During her work at ERA, she led numerous independent safety assessments in a range of sectors including oil and gas, defence, medical, nuclear, air traffic control and railway protection systems. She also set up and led two multi-million-pound collaborative research projects on safety-critical systems, one for industrial data driven systems and the other in machine learning. In 1997, Audrey set up Virkonnen, specialising in safety-critical computer applications and consultancy, an undertaking monitoring and assessment activities for government funded research. In more recent years she has acted as Engineering Safety Manager for the Piccadilly to Heathrow Line, Northern Line Signalling upgrade and a Northern Line Extension to Battersea Power Station.

Her professional activities have included being a member of the IET Council, chair of the (IEE) software engineering professional group, member of the Control and Automation Board and founder and past chair of the IET Safety Community, Engineering and Physical Sciences Research Council (EPSRC) advisory and NATO standardisation boards. In 2016 she was awarded the IEC 1906 medal recognising exceptional current achievements. In 2020 she was appointed to the Joint ISO/IEC Working Group developing standards in AI. She is currently co-chair of the IEC 61508 committee and the international lead on functional safety on the Advisory Committee on Safety (ACOS) to the IEC Standards Management Board.

She has published more than 20 papers, her most recent being 'Functional Safety, where have we come from, where are we going?' (SCSC, 2017), 'Developing Safe and Secure Standards' (IET, 2017)' and 'Safety through Systems using Artificial Intelligence', Vision Zero Summit, Japan 2022.

Yvonne Oakshott

Yvonne has worked in the defence aerospace sector for four decades, and at Leonardo Electronics for a long time. There, her current role is as a technical leadership executive and an Independent Technical Authority, responsible for the safety, security and integrity of their products.



Merlin Helicopter

Yvonne's specialist areas of expertise are airworthiness related programmable element assurance and system safety for future systems / new technologies.

She also possesses in-depth knowledge of aircraft systems, safety of weapons systems, systems and product safety, flight safety / airworthiness, recent developments in airworthiness cybersecurity, platform and subsystem safety cases (monolithic and modular), embedded software development and risk-based assurance.

Her career began as an embedded software engineer in Leonardo Helicopters (formerly Westland Helicopters) and she has worked her way up to where she is today. She successfully provides independent assurance in support of design certification and operates in a consultancy role as a subject matter expert to provide guidance to development teams. She speaks with confidence on regulatory matters, safety, programmable element (Software and Hardware) assurance, governance and certification. She is a representative on Leonardo's software process group and chairs the forum for the product technical authorities, and currently works with functional heads to develop proactive approaches to assure the safety of programmable elements across the company.

Throughout her career, Yvonne has contributed to the success of a wide variety of commercial and research-based programmes, interacting with customers, industry representatives and academia.

Yvonne is Vice Chair of the strategic Defence System Safety Group (DSSG), an important group whose purpose is to advance safety practice and safety governance of defence systems by representing the consolidated views of the UK defence industry.

As a long-term member of the SCSC Assurance Case Working Group, Yvonne also provides expert input into industry guidance. To date she has authored four safety-related conference papers.

She has been a co-recipient of BAE and Leonardo Industry Awards for her safety related research work, she is a great role model for women and passionate about helping and developing those looking to follow a technical career path

Outside work, Yvonne has a long association with archery and during the 1990s was ranked one of the top four ladies in the UK!

Zoe Alderman



Zoe did not have a traditional route into engineering; her first degree was in Politics, followed by a postgrad in History and Education (whilst also running a pub and restaurant). She had always wanted to be a history teacher (or possibly a writer for Private Eye) so it came as a bit of a shock to realise that she wasn't actually very good at it; she helped children pass exams but was unable to inspire them with a love of the subject and gained much admiration for those who do it their whole lives.

While mulling over her options, she went temping at a local engineering company, Westinghouse Signals (now Siemens), and there discovered a world she hadn't realised existed. She lasted one day on the photocopying, then went to find something more interesting to do. In her first year there she helped write maintenance manuals, tried requirements traceability, wrote interface specifications, searched out supporting evidence for contractual variations, and did software testing. She was then offered a job in the safety team and sent back to university for a third time, to do an MSc in Safety Critical Systems Engineering. The team she joined were endlessly supportive as she worked her way through the skills of RAMS engineering, and she ended up specialising in safety cases.

Zoe finds great joy in pulling together the strands of evidence into a logical argument and establishing the limitations of that argument. She is a clear advocate of safety being a lot more than just understanding failure modes and their impact on systems; safety engineers have to extract information from experts, need to manage change to improve processes, create logical arguments that need sufficient depth to inform readers without blinding them with detail, and need to have the conviction in their work to hold firm when others try to cut corners. They also need to be open to questioning of their work, without taking it as a personal slight, and acknowledge errors when they have been made.

After nearly two decades at Westinghouse, Zoe moved into contracting to enable her to work more flexibly around family commitments. It also enabled her opportunities to travel, including Korea, Hong Kong, Sweden, USA and Canada. This enabled her to work with a whole variety of safety cultures and processes, alongside different technologies.

Zoe has an abiding love for the London Underground, from its grimy beginnings to its sparkling new stations, and was fortunate to lead the safety team that delivered the first stages of the Victoria Line signalling system into service. Her last job saw her back at Westinghouse/Siemens, which was a challenging role on the Crossrail SCADA project and was the most fun she had had in a long time (it being a hugely demanding project with tight deadlines, brilliant co-workers, and enormous complexity!) After Crossrail, Zoe decided that she would take the Gap Year that she could never afford when she was younger. At time of writing, she is still on sabbatical, but intends to return if the right job arises. Preferably underground!

End Notes

It is worth reflecting in today's safety world of concerns about AI that Ada speculated that Babbage's machine was "*a thinking or ... reasoning machine*" but warned "*It is desirable to guard against the possibility of exaggerated ideas that arise as to the powers*" [of the machine]. Wise words from the 19th century indeed.

My own interest in Ada Lovelace began a long time ago as I'm a former pupil of the same secondary school that Babbage attended, and so I became aware of her at a young age. I was also in the second year ever of 'O Level' Computing and one of only two or three girls in my year to take it. I learnt to program in a few computer languages, mostly C and FORTRAN, but ironically can't claim to have learnt ADA, nor subsequently become a software engineer, being more interested in physics, the hardware and other forms of engineering. I do however suspect that my life would have turned out differently if I hadn't known about Ada back then, as she was an ever-present inspiration throughout my school years.



Blue plaque, St James Square, London

References

[1] Ada Lovelace Day – Celebrating the achievements of women in science, technology, engineering and maths: www.findingada.com, accessed Sep 2023.

[2] Key Women of Newstead Abbey - Newstead Abbey, https://newsteadabbey.org.uk/key-women-of-newstead-abbey, accessed Sep 2023

[3] The Thrilling Adventures of Lovelace and Babbage: The (Mostly) True Story of the First Computer, ISBN-10: 9780141981536, Syndey Padua, 2016.

Image attribution
Top image: , Creative Commons https://commons.wikimedia.org/wiki/File:Ada_Lovelace_1838.jpg, public domain
Analytical Engine: https://commons.wikimedia.org/wiki/Category:Analytical_Engine#/media/File:Babbages_Analytical_Engine,_1834-1871._(9660574685).jpg, CC-BY-SA 2.0
Newstead Abbey: https://en.wikipedia.org/wiki/Newstead_Abbey#/media/File:Newstead_Abbey_from_Morris's_Seats_of_Noblemen_and_Gentlemen_(1880).JPG, Public Domain
Ada logo, Public Domain | Audrey Canning at the Worshipful Company of Engineers © Audrey Canning | Merlin https://en.m.wikipedia.org/wiki/File:Royal_Navy_Merlin_Helicopter_MOD_45155806.jpg (OGL v1.0).
Zoe Alderman profile, © Zoe Alderman
Ada Plaque: https://en.m.wikipedia.org/wiki/File:AdaLovelaceplaque.JPG, e Creative Commons Attribution-Share Alike 3.0 Unported

Wendy Owen

Wendy has nearly 35 years' experience in systems assurance across a wide range of highly regulated industries covering energy, defence, transport and process sectors. Her career has largely been in engineering consultancy, also with time in product development, research and regulatory. She is a Fellow of WES and the Safety & Reliability Society, and within SCSC a task lead in the Security Informed Safety Working Group (SiSWG) and a member of the Steering Group. Wendy is also the DEI (diversity, equity, and inclusion) lead for the SCSC.

This article is dedicated to Maria, who was the first person at her university to combine computing and fine art, nowadays a strategic CTO, long time BAFTA judge and STEAM advocate.

The author retains copyright of this article.

Seminar: What Makes Good Evidence for a Safety Case?

"This seminar is for all those who have to develop or review safety or assurance cases, including safety engineers, safety managers, consultants and regulators".

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

What Makes Good Evidence for a Safety Case?

Thursday 30 November, 2023 - Wellcome Collection, London

This seminar will examine the role of evidence in supporting a safety case. What makes strong, compelling evidence - and what is weaker evidence? If evidence is not available or is of poor quality what can be done to make up the gaps? If evidence is continually evolving or being updated how should this be handled?

Different types and characteristics of evidence will be highlighted, and their advantages and disadvantages discussed.

Speakers include:

Norina (Popa) Ratiu, Oxbotica - *TBA*

Sean White, NHS England - *"Addressing the Challenges of Evidence in Healthcare IT"*

Helen Wright, ARC Ltd - *TBA*

Sarah Tovey, MOD - *TBA*

The event will start at 0930 and finish about 1700. Further details TBA.

This event will be held in-person at the Wellcome Collection, 183 Euston Road, London NW1 2BE. This is a fabulous venue with many things to see in free exhibitions.

Your Ad Here!

Do you have a product, service or event you would like to advertise in the Newsletter? The SCSC Newsletter can reach out to over 4,000 individuals involved in Systems Safety and so is the perfect medium for engaging with the community.

For prices and further details, please get in touch with the Newsletter Editor.

Software in Railway Applications



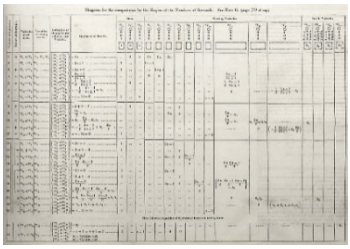
In this modern era, software is embedded in all aspects of our life. Without software, our lives would be completely different. Can you imagine your typical day without a smartphone or laptop? Even in our cars and trains, software is essential to functions and services for both drivers and passengers. So, what is software? How do we ensure it is fit for its intended use? And, how do standards help us do this?

Lucia Capogna answers these questions, provides an overview of software standards in rail and their evolution, and discusses the latest developed software standard for railway applications. Lucia will explain the significant changes, the additional guidance on lifecycles and model-based design and how some requirements have been rewritten to aid interpretation and understanding. She has also interviewed two members of the CENELEC WG28 on their thoughts about the new software standard and the future of software.

Note: the first part of this paper provides background for those less familiar with software and the current railway standards for software; the second part covers recent developments in more detail.

Software – history, definition and main characteristics

The first electronic stored-program digital computer was realised in 1951 with the Electronic Discrete Variable Automatic Computer (EDVAC). The idea of programming was first established over 100 years earlier in 1843, when Ada Lovelace (who worked closely with Charles Babbage) published the first computer program (an algorithm to calculate a sequence of Bernoulli numbers).



Ada Lovelace is still considered the founder of the discipline. The first person that really came up with a software theory was Alan Turing in 1935, and it is from there that both computer science and software engineering disciplines originated.

Since then, software started becoming popular and making inroads everywhere including the railway industry. But what is software?

The International Electrotechnical Vocabulary (IEV) [12] defines software as:

"assembly of programs, procedures, rules, documentation and data, pertaining to the operation of an information processing device or system.

Note 1 to entry: Software is an intellectual creation that is independent of the medium upon which it is recorded.

Note 2 to entry: Software requires hardware to execute programs, and to store and transmit data."

"Software requires hardware to execute programs, and to store and transmit data."

(Note 2 of IEV ref 171-01-21)

Software is something intangible (it cannot be hit by a hammer) that does not exist alone and, for this reason, it cannot cause damage on its own. It has a large list of advantages including flexibility and scalability, cost-effectiveness, fast response to issues and it is indefinitely replicable (cheap) especially on large scale projects where it can be uploaded and changed on multiple systems in parallel. However, software is context dependent, can have a large number of failure modes and it is impossible to test exhaustively (it cannot be demonstrated to be 'bug' free).

The need for a structured approach

As you may know, software is subject to systematic failures only, so a qualitative approach must be considered.

Software has gradually changed the face of railway as numerous command systems, both safety and non-safety related, have been innovated, become more flexible and evolved thanks to the use of software.

Over the years, in the Rail industry, as well as other industries with safety critical control systems, we have seen incidents caused by software failures. How do we ensure the software is fit for its intended use? In particular, how do we do it for safety related software?

Root cause analysis and incidents investigations have identified poor management in several areas across the software lifecycle starting from the requirements management, testing, verification and validation, but also lack of recording and management of change. More guidance and a more structured approach for software assurance was needed through further standardisation, and adoption of improved procedures and guidance. The more general importance of standards has been discussed in more detail in the SSS'23 paper "Making the Safety Standards Work for You" [1].

Rail Software Standards – Their history

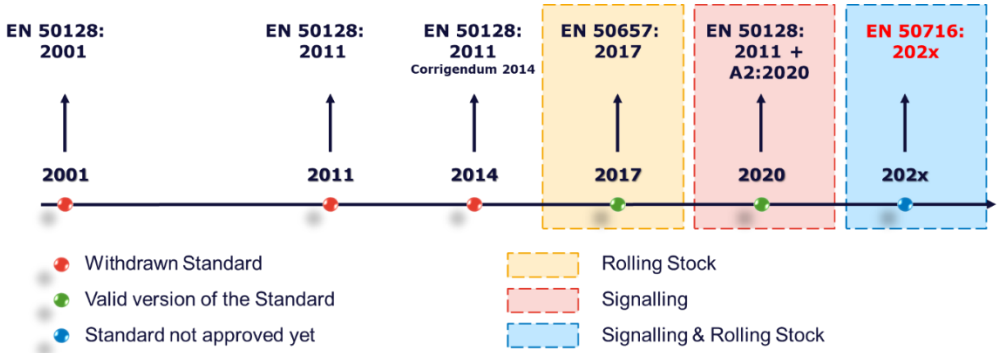
To answer the need of having common rules when developing software for railway applications, a group of experts representing different stakeholders across the rail industry and several European countries, worked together to create the first software standard for railways applications: "EN 50128:2001 – Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems" [3].

This standard follows a top-down approach to identify suitable methods for software development depending on the integrity required. It addresses 5 software integrity levels, SIL 0 to SIL 4, where 0 is the lowest and 4 the highest. The higher the risk resulting from software failure, the higher the software integrity level needs to be.

This standard has been gradually adopted by the industry and stayed unchanged for 10 years, until an updated version of the same standard was developed and published (EN 50128:2011). The 2011 version has been greatly improved thanks to the return of experience from the industry; it has adopted a new structure that has remained stable since then.

For over 16 years the EN 50128 (in its different versions) has been the software standard used by both Signalling and Rolling Stock, despite the fact it was specifically developed for signalling and protection systems. However, in 2017 a dedicated software standard for Rolling Stock was published: "EN 50657:2017 – Railways Applications – Rolling stock applications – Software on Board Rolling Stock" [5]. The EN 50657:2017 adapted EN 50128:2011 requirements for the application of software in the Rolling Stock domain and aligning it to the principles and terminology used in the new EN 50126 series [9]. [10] (published in the same year, 2017). From now on SIL 0 is replaced with Basic Integrity (BI).

TC9X WG28 received the mandate to update EN 50128:2011 [4] to align with other standards in the railway framework (i.e., EN 50126-1:2017 [9], EN 50126-2:2017 [10] and EN 50129:2018 [11]) resulting in the EN 50128:2011 + A2:2020 [6] published by The British Standards Institute (BSI) in August 2020. This has been a first step towards the development of a new software standard applicable to both Rolling Stock and Signalling: FprEN 50716 [7]; this standard is currently under final vote and it is expected to be formally published before the end of 2023.



FprEN 50716 Improvements and changes – Open discussion with key people in the CENELEC Standardisation group (WG28)

The FprEN 50716 standard [7] will supersede the latest EN 50128:2011 [6] and EN 50657:2017 [5] and all of their amendments and corrigenda, hence it is applicable for both Signalling and on-board Rolling Stock. For railway related fixed installations (electric traction power control and supply) "EN 50562:2018 - Railway applications - Fixed installations - Process, protective measures and demonstration of safety for electric traction systems" [8] remains applicable.

FprEN 50716 [7] includes several significant technical changes with respect to the latest EN 50128:2011 [6] and EN 50657:2017 [5]. The new software standard is now fully aligned with EN 50126-1:2017 [9] and EN 50126-2:2017 [10] terminology and definitions, and many requirements have been re-written to simplify and clarify them (e.g. organisation requirements); the techniques and measures have been better aligned with the lifecycle phases, and generalised where appropriate (e.g. programming languages). This standard now offers guidance on several lifecycle models and on modelling for software development as many software projects are now using modelling and model-based design. The emerging use of Artificial Intelligence (AI) and Machine Learning (ML) is also discussed and recommendations and guidance from a previous version of EN 50128 have been reviewed and updated in the new standard. Although many areas have been improved or added, the core requirements of the existing software standards stayed nearly unchanged. Those requirements are already clear and left untouched as they are good principles across the software development processes.

The author interviewed Andrea Palermo and Attilio Ciancabilla to discuss the changes introduced in the FprEN 50716 [7], the challenges faced when developing the new standard and the future of software in railway applications.

Andrea Palermo is the Convenor of WG28 for the new FprEN 50716 [7] (UK National Committee). He is also involved in other CENELEC and IEC safety standardisation working groups. Andrea works in Thales GTS, defining digital solutions for the UK mainline railway.

Attilio Ciancabilla is an active member of WG28 for the new FprEN 50716 [7] (IT National Committee). He is also involved in other CENELEC and IEC safety and cybersecurity standardisation working groups. He is the convenor of WGA15, in charge of maintenance of EN

50129. Attilio works in RFI (Rete Ferroviaria Italiana) in the signalling field, mainly for electronic interlocking systems.

I asked Andrea, what it meant for him to lead the group developing a new software standard to be used for both Rolling Stock and Signalling, and what challenges / rewards he had from the experience but also if he would change anything that has been done.

Andrea said that the 2001 version of EN 50128 really transformed the way software was developed for signalling applications and through the years became a best practice used for overall assurance (beyond safety) and cross domain, so when a mix of experts started working together on the FprEN 50716 [7] they all had a common language and understanding! Andrea also clarified that it was immediately clear that while the majority of needs were common, significant differences existed: his role was to lead the group in finding the right compromises.

One of the biggest challenges for Andrea was to lead the group during the COVID-19 pandemic, however he has seen this "low" point as an opportunity to "virtually" work together more frequently than what would have been possible with in-person meetings, transforming it into a "high point". Andrea went through the steps made in the last few years, from the work done in the survey group that produced a baseline draft merging EN 50128 [6] and EN 50657 [5] with agreed trade-offs between all experts and explained that this impacted on the direction the standard has taken. After that, the "mantra" of the working group was to keep continuity from EN 50128 and EN 50657 and facilitate transition – they even kept the majority of the numbering of clauses unchanged in this respect to minimise traceability updates. The choice was made consciously, but he underlined that if they would have gone for a thorough review from first to last page, the standard would have been much different.

I asked both Attilio and Andrea their opinion on the direction the software standard is taking and their thoughts regarding the use of new "technology" or "approaches" like AI and ML and how standards may need to evolve to accommodate cloud-based solutions.

The standard kept the usage of AI and its derivatives like ML open for basic integrity (it is not recommended for SIL 1 – SIL 4) but Andrea expects that in the coming years, these techniques will be used also as sorts of "support tools" to gain additional confidence in software verification and validation (the standard does not preclude this as it defines the "what" not the "how" in term of development process). The next revisions of the standard will probably expand on AI topics over the coming years, also taking benefits from the broader standardisation efforts on-going in IEC/CENELEC.

Overall, both Andrea and Attilio agreed that merging the two existing standards into one has been a great achievement considering the different needs, but also, that we work in an integrated context. Attilio has a long history in the standardisation environment, and he is quite sure that in a not-too-distant future we will be able to extend the standard to fixed-installation applications as well.

"Leading the WG28 was such an enriching experience! {..} finding the right trade-offs has been probably the most rewarding part of the work."

Andrea Palermo (Convenor of WG28)

Attilio said that, in his opinion, another big improvement has been simplification: requirements on roles have been clarified, approach to programming languages was obsolete and has been changed. In general, we can say that the standard is now more flexible and less constraining, which will make it easier to use.

Attilio also said that cloud computing is in our future. Railway applications are characterised by relatively slow real time processes, so he does not think it will be difficult to guarantee high available, fail-safe and secure cloud computing. But for adequate fault tolerance he also believes that there will be a need for some local element able to manage the so-called "graceful degradation", and this architectural challenge will perhaps be the most difficult to solve.

At the end of this interesting discussion, I asked Attilio what he thinks will be the impact of this new standard on the industry also considering its relationship with other existing standards like EN 50126, EN 50129 and the TS 50701. Attilio said that it is always difficult to consider the relationships between standards and their inter-applicability and despite the great work that has been done to align the EN 50716 to the EN 50126 and EN 50129, there is still room for improvements (e.g., requirements on tools). He concluded that differently from EN 50129 and from the latest EN 50128:2011 [6], this new software standard will extend the scope to non-safety-related software. Attilio is afraid there will be some resistance in adapting to this, but on the other hand this will facilitate the homogenisation of developing processes and will eventually be seen as an advantage.

Cambrian Coastline incident and RIS-0745-CCS

The Railway Industry Standard RIS-0745-CCS [12] has been produced by The Rail Safety and Standards Board (RSSB) to support Network Rail (after the Cambrian incident [2]) and the rail industry in general. It gives guidance and sets requirements regarding safety assurance activities for the client's organisation responsible for the procurement and use of safety-related software-based systems. It heavily refers to the EN 50126/8/9 standards. The client's role in safety assurance is defined at the level of the whole system under consideration. When a high integrity software-based system is procured, the client organisation is the relevant Railway Duty Holder under the relevant regulations.

The focus of this standard is to ensure that the software within high integrity software-based railway systems does not cause hazards and it is less focused on the in-depth analysis of the actual activities to develop and maintain safety-related software-based systems. The RIS-0745-CCS [12] clarifies the responsibility of the client organisation in meeting the requirements of the suite of railway software standards; it provides them with increased confidence that the requirements of the suite of railway software standards and the CSM-RA (Common Safety Method for Risk Evaluation and Assessment) have been met by requiring further specific activities.

Conclusions

An increasing portion of the railway functions (safety and non-safety related) are being supported by software.

The risk associated with the use of software in the safety context has led to the need for more guidance, procedures and standards to increase the quality of the software and to assure that the risk is reduced to a tolerable level.

The newly developed cross-domain standard (FprEN 50716 [7]) improves readability of the requirements and gives more guidance on several aspects compared to the two existing software standards it will supersede (EN 50657 [5] and EN 50128 [6]). It is also more flexible and less constraining, which will make it easier to use.

"The role of a standard such as EN 50716 is to follow innovation, providing minimum requirements on objectives and processes.

Attilio Ciancabilla
(Convenor WG15 and member of WG28)

Software is so embedded in railway functions that the RSSB created an industry standard to support software assurance from the client perspective (RIS-0745-CCS [12]) aiming to reduce risks associate with its use.

Compliance to standards gives reassurance and increases confidence that the software is fit for its intended use and that its quality is adequate for the identified safety integrity level. These methods support a structured and consistent approach in the development, verification and validation of the software and its use across different organisations and countries.

References

[1] SSS23 Bull, Capogna, Davies & Gill – Making the Safety Standards Work for You, Feb 2023

[2] RIAB, Dec 2019, "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017".

[3] CENELEC, EN 50128:2001, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[4] CENELEC, EN 50128:2011, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[5] CENELEC, EN 50657:2017, Railways Applications – Rolling stock applications – Software on Board Rolling Stock

[6] CENELEC, EN 50128:2011 + A2:2020, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[7] CENELEC, FprEN 50716, Railway applications - Requirements for software development

[8] CENELEC, EN 50562:2018, Railway applications - Fixed installations - Process, protective measures and demonstration of safety for electric traction systems

[9] CENELEC, EN 50126-1:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[10] CENELEC, EN 50126-2:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[11] CENELEC, EN 50129:2018, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

[12] RSSB, Rail Industry Standard, RIS-0745-CCS, Client safety assurance of high integrity software based systems for railway applications

[13] https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-01-21, accessed, Sep 2023

Image attribution
top image ID 210738093 © BiancoBlue | Dreamstime.com
Diagram for the computation of Bernoulli numbers © Public Domain | https://en.wikipedia.org
Standards Timeline © Lucia Capogna

Lucia Capogna, Principal Engineer, Ebeni Limited

Lucia has over 15 years' experience in software, safety and cyber security with background in multiple industries including Railway, Defence, Oil & Gas and Renewable Energy. Lucia also represents the UK in several CENELEC and IEC standardisation groups (UK NC) for software, cybersecurity and safety standards, including WG28 (FprEN 50716).

The Data Risk Zoo



In the October 2022 edition of the SCSC Newsletter, the authors introduced the concept of a "Data Risk Cygnology" that categorised types of *data safety risk*. Here they discuss further ideas in this area and work towards a more formalised taxonomy of terms.

Classifying data safety risks can help tease out some unlikely but severe failures of systems involving data. It is possible that sometimes these risks are already considered in system hazard analysis sessions but discounted as too unlikely to happen. We believe that having a more formalised and visual approach provides a useful "Tool in the Box" when trying to identify extreme data-related risks of systems. Due to their serious impact, we believe that they should be included, assessed and managed alongside more "normal" risks.

In our 2022 article we defined four new classifications of data safety risks:

1. Black Swan Data
2. Perfect Storm Data
3. Dragon King Data
4. Pudding Lane Data

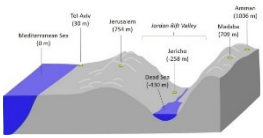
Since then, we have identified many other different types of data safety risk, some new and some variants of others. These broadly fall into three general categories:

- Dead Data
- Hidden Data
- Legacy or Change-derived Data.

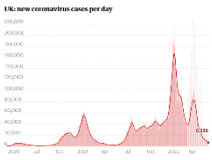
In this article we describe some of these new concepts and our proposed classification model to help corral the emerging "zoo" of data safety risks.

Data Risk 'Cygnology'[1]

The following table shows the original classification terms introduced in the previous article, the imagery that was developed and a reference to an example accident.

Type	Brief Explanation	Real-life Example
 **Black Swan Data**	*Data that is totally unexpected by those receiving it (i.e. 'out of the blue') and has huge (detrimental) impact, but in retrospect should have been anticipated.*	In 2013 a C-130 Hercules aircraft landed at Bar Yehuda airport near the Dead Sea [1], a saltwater lake astride Israel and Jordan. The airfield lies 1,210 feet below sea level.  The plane's navigation electronics were not designed to operate at altitudes less than 400 feet below mean sea level.
 **Perfect Storm Data**	*Combinations, sets or occurrences of data (or sets of absences of data) that would never have been thought possible to occur together, and when they do, have a large and undesirable impact.*	China Airlines A333 at Taipei on 14th June 2020 [2] when all primary computers, reversers and auto brakes failed on touchdown. 
 **Pudding Lane Data**	*Data that is unknowingly and unexpectedly critical to the whole operation and if missing or incorrect in some way, has a dramatic and negative impact. After the event it may be obvious that it was critical.*	 In 2015, an Airbus A400M on a test flight crashed with reports suggesting that as many as 3 of the aircraft's 4 engines failed during departure from Seville [3]. The reported cause of the failure was the torque calibration parameter data being wiped on 3 engines as the engine software was being installed, stopping the software from operating properly. In this case, the seemingly innocuous calibration data had a critical role to play in the safety of the entire platform.

[1] This is the term used in Risk Management for these types of risk

Type	Brief Explanation	Real-life Example
 **Dragon King Data**	*Data that might have been foreseen, but leads to an unexpected and explosive escalation with major impact ('things get rapidly out of control').*	 The loss of data relating to Covid-19 test results in the UK due to a row limit in Microsoft Excel led to the loss of 15,841 positive test results, which in turn meant that 50,000 potentially infectious people were missed by contact tracers and not told to self-isolate [4]. Because of the exponential way that viruses spread, this may have led to many more infections and deaths.

It is noted that the recent flight plan outage at NATS [7] which led to a week of flight disruptions, cancellations and delays, and cost approximately £300m in extra costs for airlines, would definitely count as one of these types above, probably Dragon King Data or possibly Black Swan Data. The knock-on effects of a small outage due to a data problem (duplicate Waypoints outside UK airspace in the flight plan) quickly escalated as the airlines had little resiliency in their operations. This incident was discussed by both the Data Safety Initiative and Safer Complex Systems working groups.

The Plot Thickens…

We don't always have the opportunity to work on new or 'green field' systems. We often need to maintain legacy systems that may have been running for many years if not decades. Imagine therefore that you have been assigned to maintain a large, complex and critical software system, which has evolved over many years. You are faced with many code modules and data files, some of which are undocumented, with the original development team long gone; you simply don't know what some of the data does in the system.

Typical problems we might see with such systems are:

- Configuration or initialisation files – what combinations of values are allowable and meaningful?
- Repurposing of database fields from their original intended use
- Translations and mappings built into the code with no explanations
- Ill-defined default values
- Special data workarounds done manually (it always does this, just enter X and carry on)
- Not all values are used or reachable ("dead")
- "Magic numbers" – literal items of unknown derivation

From these examples, we can draw three new classifications of data safety risk:

- **Dead Data**: data that is not, (or thought not to be), available or used – but in some cases should be
- **Hidden Data**: data which is intentionally or mistakenly concealed or hidden
- **Legacy or Change-derived Data**: data that is related to change and evolution of systems.

Dead Data

Data that is not, (or thought not to be), available or used – but in some cases should be

Computer science has had the concept of "Cruft" since at least the 1950's and is defined in Wikipedia [5] as:

anything that is left over, redundant and getting in the way. It is used particularly for defective, superseded, useless, superfluous, or dysfunctional elements

There are analogies in the aviation world, for example, the software assurance guidance for airborne systems (RTCA/DO-178C) describes the need for consideration and handling of:

- **Deactivated Code**: code that cannot be executed, such as unselected functionality or unused library functions, or data that is not used
- **Dead Code**: Executable Object Code (or data) which exists as a result of a software development error, but cannot be executed (code) or used (data) in any operational configuration of the target computer environment

We therefore can draw these ideas into the data world by defining the general class of **Dead Data** and a subtype of Dead Data called **Deactivated Data:**

- Data intentionally unused due to current configuration of the system
- However, it could be used due to a reconfiguration, system change, change of use, or a failure
- The data may be used in the wrong configuration (or if the deactivated configuration fails to be tested) when there are functional changes

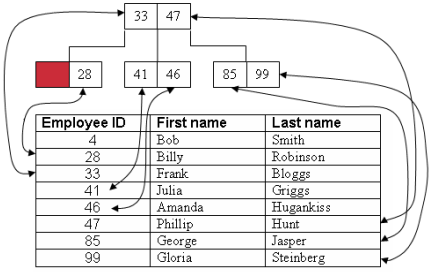
```
a=10;
if mode is "debug" then
   a=100;
```

Hidden Data

Data which is intentionally or mistakenly concealed or hidden

Data might exist in a system but the method of access: e.g. index, map or hash table has become lost or corrupted and so there is no easy way of getting access to the data.

In the example opposite, the loss of an intermediate index node might make it impossible to find the attributes for a given search key (Id=4).



Employee ID	First name	Last name
4	Bob	Smith
28	Billy	Robinson
33	Frank	Bloggs
41	Julia	Griggs
46	Amanda	Hugankiss
47	Phillip	Hunt
85	George	Jasper
99	Gloria	Steinberg

We therefore define this as a subtype of Hidden Data called **Treasure Island Data**

Data may also be concealed intentionally within other data and might even be considered "half-dead" if you know how to find it. Examples of this are hidden messages or watermarks in pictures and we use the term **Steganographic Data** for this type of Dead Data.

Legacy or Change-derived Data

Data that is related to change and evolution of systems

Systems that have been in service for long periods are often changed over time by different people and the 'memory' of the original purpose and intent of the data can be partially or fully lost. Sometimes there is a desire to modernise the system with new contemporary systems that have different models for managing the data. However data doesn't therefore always map or fit in a field, it may be mapped incorrectly, lost, truncated or set to a default or null value.

Consider the following healthcare example, where a legacy text-based prescription system is being replaced by a new digital system where the number, type and frequency of medication dosage is held in specific fields. This translation works for most until we encounter a PRN instruction (Pro Re Nata – "as and when required"):

Old system (text)

Medication Description
25 ml twice per day
1 tablet once per day
1 tablet PRN



New system (digital)

Num.	Type	Freq.(hrs)
1	25 ml	12
1	tablet	24
How to represent PRN?		

There is no obvious translation for this, and so special provision will need to be made and this subtlety may be lost in the migration process.

In a sense this is trying to squeeze data into something it doesn't fit and so we define the term **Square Peg Data** for this class of data problem.

"Magic Numbers" were mentioned earlier and defined (amongst others) in Wikipedia as:

- A unique value with unexplained meaning or multiple occurrences which could (preferably) be replaced with a named constant

The use of magic numbers can result in the provenance of the data being lost and hence it is difficult to verify that the value is correct and continues to be correct. (e.g. an unexplained value of 365 will be incorrect 25% of the time if it is actually representing number of days in the year, due to leap years).

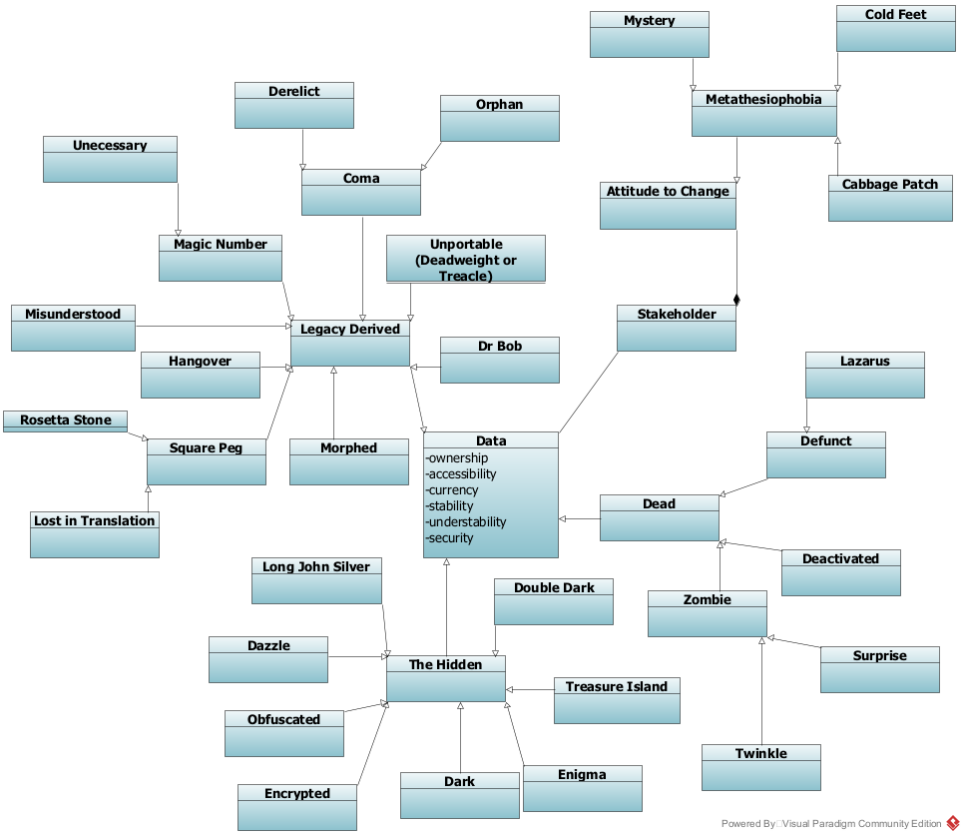
```
clear all;clc;
%Simulation of Transformance Performance
zw=4+5*i;
zl=80:10:200;
V1=220;
V2=V1/0.5;
I2=V2./zl;
n=(V2.*I2)./((V2.*I2)+(I2.^2)*4+40);
xlabel('Load')
ylabel('Efficiency')
title('variation of efficiency with loadi
plot(zl,n)
```

If the value is also used in different places, then it will be duplicated, which places a burden on the developers to ensure the values are all consistent. If the value does need to be updated, then the system may become inconsistent unless all cases are found. We therefore define the term: **Magic Number Data** for this type of data risk.

Even if good practices are adopted and literal constants are used instead of hard-coded values, then it is possible that new literal constants are introduced into a system during maintenance, when an already-defined constant should have been used (usually because the maintainer is unaware of the previous definitions). For this scenario, we define this sub-type of Legacy or Change-derived Data as **Unnecessary Data.**

Zoo Keeping

As the number of different terms expand, it is useful to try and corral these and identify the relationships more visually. The following taxonomy has been developed to encompass all the terms identified so far.



The following table describes the other terms not already covered.

Dead Data Subtypes

Name	Explanation
Defunct Data	Data that may have been initially used in the system by design, but subsequent changes make the data unneeded, unreachable or unusable.
Lazarus Data	Data that should not be defunct, i.e. it is currently unused due to a mistake (e.g. incorrect change applied), but actually should be currently used, incorporated or available within the system.
Deactivated Data	Data intentionally unused due to current configuration of the system. However, it could potentially be used due to a reconfiguration, change, planned reactivation or a failure. There are therefore risks if the data is used in the wrong configuration (or if the deactivated configuration fails to be tested) when there are functional changes.
Zombie Data (Undead Data)	Data thought to be defunct but in fact is used, (perhaps in an obscure way), perhaps in parts of the system rarely used.
Surprise Data	Data that is assumed lost, deleted or unavailable but can resurface and become unexpectedly available when conditions arise.
Twinkle Data	Data that is temporarily unavailable or intermittently available for whatever reason, on a regular or irregular basis.

Hidden Data Subtypes

Name	Explanation
Treasure Island Data	Data to which the method of access (e.g. index, map or hash table) has become lost or corrupt so that, although the data still exists, there is no easy way of finding it (or getting to it).
Enigma Data	Data to which the encryption key or keys have become lost so that, although the data still exists, there is no way of decrypting it.
Steganographic Data	Data that is concealed intentionally within other data.
Encrypted Data	Data that is specially coded and only accessible using a key or keys.
Obfuscated Data	Data that is purposely made difficult to understand, read or use.
Double Dark Data	Data you are not aware of and have no idea what it does, and therefore cannot be changed intentionally. However it may be changed by mistake and have significant effects on the system. For example, deleting an empty folder that contains a hidden configuration file used by the system.
Dark Data	(Requires further work on Dark Data types).
Dazzle Data	(Requires further work on Dazzle Data Types).

Legacy or Change-Derived Data

Name	Explanation
Square Peg Data	This is data where on migration or on translation between systems data doesn't map to a sensible new category or type, or doesn't fit in a field width, so it is mapped either to something which is not quite right, truncated or set to a default or null value. I.e. you are trying to squeeze it into something that it doesn't quite fit, and losing information in the process.

Name	Explanation
Rosetta Stone Data	1-1 mapping could exist but has to be identified or defined.
Lost in Trans-lation Data	No 1-1 mapping exists – some fudging has to be done, or data has to be rejected.
Coma Data	Data that is unused for now, and as such never gets updated as it should to current values or formats. If it is ever used (e.g. due to change, system re-configuration, or change of use) it may therefore present a problem.
Derelict Data	Data that is known about but has not been updated / maintained and is no longer fit for purpose, and so is 'worked around' (e.g. overridden) at every use or invocation of the system.
Orphan Data	Data that is in current use but no longer has an owner or sponsor so may never be maintained or updated.
Hangover Data	Legacy data that has been left over from installations or previous versions of the system and should not be needed or used, but it may be.
Magic Number Data **(Disassociated Data)**	Data that is rarely changed and is replicated and distributed throughout a system (typically obscure numbers in software or configuration files). These items of data should in fact all refer to the same value or set of values. Because it is duplicated, individual updates can be applied and the system becomes inconsistent.
Unnecessary Data	This is where new literal constants (numbers, strings) are introduced into a system during maintenance or upgrade, when in fact an already defined constant value should have been referenced. The person adding them is usually unaware of the previous definitions.
Dr Bob Data	Data, often obscure values found in software files, which nobody in the maintaining organi-zation knows the source or derivation.
Unportable Data (Deadweight or Treacle Data)	Data that, for whatever reason (e.g. derivation is unknown or doesn't work in new schema), cannot be ported or migrated to a new system and therefore is left out.
Morphed Data	Data that originally had a defined single purpose or set of purposes, but has since been re-used and re-purposed so that it may be influencing many more things and you don't know what it impacts.
Misunderstood Data	Data you are aware of and think you know what it does (but actually you don't), therefore any changes made may be incorrect and cause problems.
Cold Feet Data	Data you are aware of and understand what it does, but are afraid to change its format or representation because you are unsure what the impact will be (e.g. update to latest schema, version of software or version of database).
Mystery Data	Data you are aware of but have no idea what it does, and therefore are reluctant to modify or update.
Cabbage Patch Data	Data where you know what it does but not why, therefore are reluctant to update. This is generally data that you don't know where it came from or how it was generated or derived so it is a matter of trust that it is correct.

Future Work



This work is still subject to ongoing development but is hopefully starting to provide some structure and insights around the many issues that can affect the data in systems and therefore different routes to contributing to safety-related hazards. The use of a taxonomy to help visualise the relationships seems useful but other methods of visualisation are possible.

In particular the "Risk Zoo" opposite [6] for standard risk management provides an effective means of showing how different types of risk relate to likelihood and severity of consequence and follows the animal theme. This particular zoo contains animals not previously considered, such as: Boiling Frogs, 800-lb Gorillas and Red Swans!

Cockroaches: events that are certain because they are pervasively present and difficult to extinguish. Because impacts are low, they are dealt with one-by-one and don't generally overwhelm the systems or people that they affect.

White Elephant: known events that we fail to act against based on the classic "elephant in the room" saying. These are big problems that we could do something about, but a combination of availability bias, optimism bias, confirmation bias, groupthink, myopia, and status quo bias can lead potential efforts astray.

White Swan: an event that is known. It is also highly certain, with occurrence that is well understood, and has a resulting impact that can be estimated easily. In short, we expect this, we understand it, we should be equipped and prepared for these kinds of events.

800-lb Gorilla: existing forces (people, businesses, governments) that can dominate the culture around them and the hands of others because of their influence and power.

Gray Rhino: a highly probable, high impact yet neglected threat: kin to both the elephant in the room and the improbable and unforeseeable black swan. Gray rhinos are not random surprises but occur after a series of warnings and visible evidence.

Boiling Frog: risks that change incrementally in time, but those changes are not taken seriously until it is too late.

Ostrich paradox (or effect): a common disaster risk metaphor used to illustrate how humans have difficulty dealing with looming disaster risk by burying their head in the sand when danger looms.

Butterfly Effect: small changes in the state of a complex systems can result in significant differences somewhere else, sometime later.

Black Elephant: a cross between a Black Swan and White Elephant where we know that one day it will have vast, black-swan-like consequences.

White Leopard: a stealthy creature that stays hidden through effective camouflage. You know it exists, but it remains hidden until it is almost too late.

White Whale: very low probability events that are known to exist as a foil to the black Swan event that is symbolic of an event that is completely surprising.

Black Turkey: an event that is everywhere in the data – it happens all the time – but to which one is wilfully blind.

Gray Swan: A rare, but known hazard, with some predictability (though perhaps not certainty), and has the potential to cascade into a high impact event.

Red Swan: a known, probable event that could create a significant impact, but eventually does not happen. These are dangerous for the future because they can erode trust between the institutions giving the warning (e.g., scientists) and the public.

We could easily imagine this 'zoo' risk model being mapped to cover data safety risks!

Work is also underway to provide more guidance and recommendations around how the risks around each item in the taxonomy can be managed. Mike and Paul would be very interested to hear from you if you would like to contribute to this novel and interesting area of research – are there more exotic animals out there we've yet to discover? Let us know!

Image attributions
Top image © Jpldesigns | Dreamstime.com
C-130: © Mr Paul Hanley | Dreamstime.com
A400M © Abhishek Singh | Dreamstime.com
Air China: https://commons.wikimedia.org/wiki/File:China_Airlines_A330-300%28B-18352%29_%285213874397%29.jpg share under Creative Commons Attribution-Share Alike 2.0 Generic license.
Covid chart: data.gov.uk published under the Government OGL license v3.0
Swan icon: © Skalapendra | Dreamstime.com
Storm icon: © Андрей Морозюк | Dreamstime.com
Pudding icon: © Amonrat Rungreangfangsai | Dreamstime.com
Dragon icon: © Kuzzie | Dreamstime.com
Index: adapted from https://en.wikipedia.org/wiki/File:Btree_index.PNG shared under Creative Commons Attribution-ShareAlike 3.0 License.
Code extract: https://commons.wikimedia.org/wiki/File:Matlab_Code_-_Variation_Of_Efficiency_Vs_Loading.jpg shared under Creative Commons Attribution-Share Alike 4.0 International license.
Risk zoo: © Yolanda C. Lin (2020). The Risk Zoo. Available at: datartathon.com/theriskzoo/
Blackett review risk classes: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/278526/12-519-blackett-review-high-impact-low-probability-risks.pdf, © Crown copyright, shared under the Open Government Licence.

References

[1] C-130 Crew Gets a Rude Shock When They Fly Their Plane Below Sea Level, https://www.popularmechanics.com/military/aviation/a26598/c-130-sea-level-dead-sea, accessed August 2022

[2] A China Airlines Airbus A330 Lost Primary Computers After Landing, https://simpleflying.com/china-airlines-a330-lost-computers, accessed August 2022

[3] 2015 Seville Airbus A400M crash, https://en.wikipedia.org/wiki/2015_Seville_Airbus_A400M_crash, accessed August 2022

[4] PHE statement on delayed reporting of COVID-19 cases, https://www.gov.uk/government/news/phe-statement-on-delayed-reporting-of-covid-19-cases, accessed August 2022

[5] Definition of "Cruft": https://en.wikipedia.org/wiki/Cruft, accessed Sep 2023

[6] Welcome to the Risk Zoo! https://datartathon.com/theriskzoo/#Welcome_to_the_Risk_Zoo, accessed Oct 2023

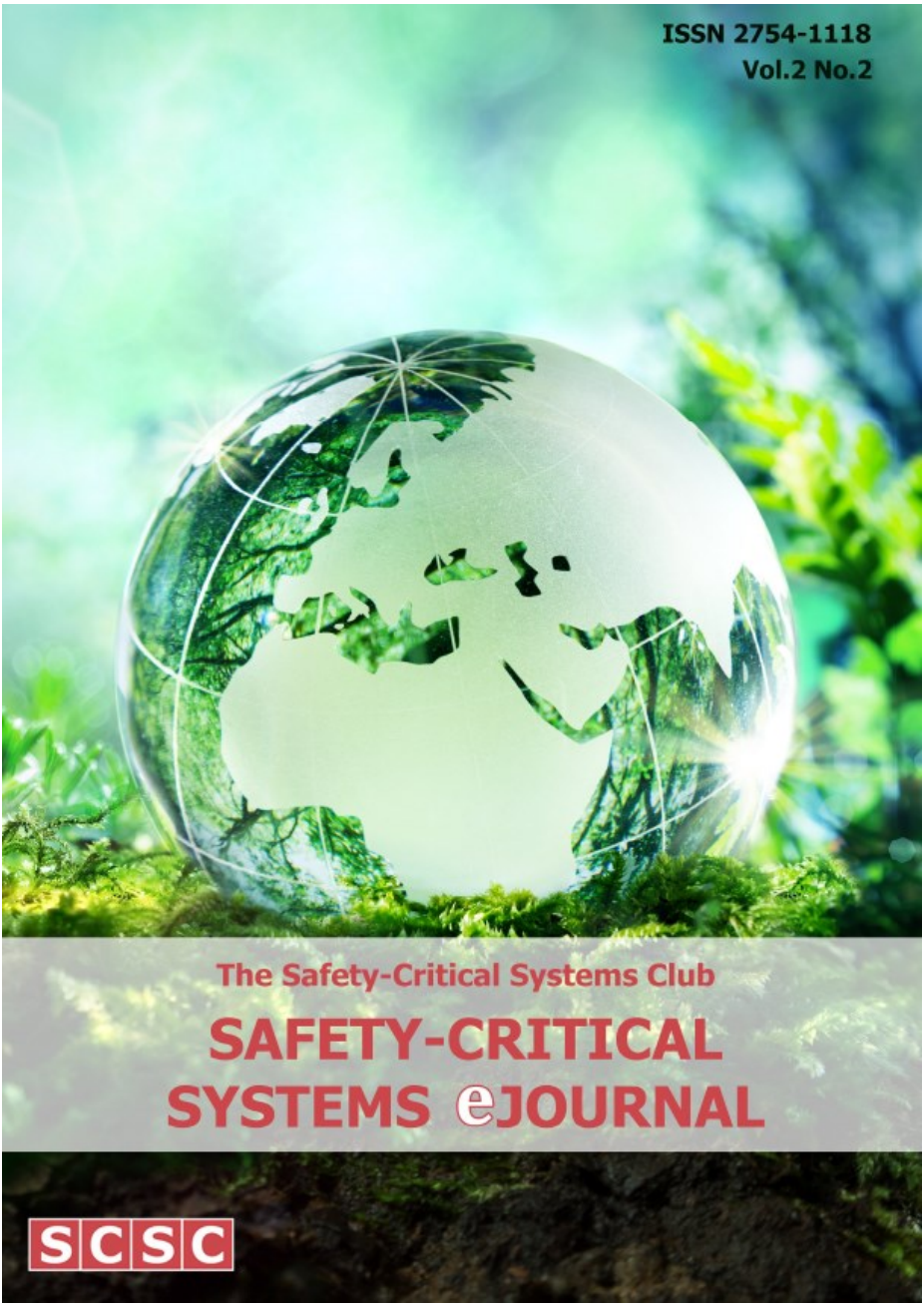
[7] Coincidentally-identical waypoint names foxed UK air traffic control system https://www.flightglobal.com/safety/coincidentally-identical-waypoint-names-foxed-uk-air-traffic-control-system/154824.article, accessed Sep 2023

Paul Hampton Safety Consultant at CGI and SCSC Newsletter Editor

Mike Parsons, Safety Consultant at Ebeni and Director of the Safety-Critical Systems Club

Paul is a Chartered Engineer with over 30 years' experience in IT. He has spent 15 of those designing and developing enterprise systems in sectors such as Energy & Utilities, Government, Criminal Justice, Health and Aviation. He has been involved in Systems Safety for 15 years in a variety of capacities including: safety engineering, safety management, independent auditing and corporate governance and assurance.

Mike has over 30 years of Safety Engineering and Management including: Development of Safety Management Systems, Assessment of Software, Services and Data Risk, Systems Safety Analysis on Development and Service Projects, Safety Assessment, Audit and Reviewing and Systems Engineering. In 2019 he became the Managing Director of the SCSC and is lead for several of the clubs working groups including Data Safety, Service Assurance and Safer Complex Systems.


ISSN 2754-1118
Vol.2 No.2
The Safety-Critical Systems Club
SAFETY-CRITICAL
SYSTEMS eJOURNAL
SCSC

scsc.uk/r186

How Do I Get Into Safety?



It is sometimes difficult to plan a career: so many things have to align together for each step on the ladder to take place, whether it is the correct training, organisation, job or assignment, or simply just being in the right place at the right time. We are sometimes asked: "how do I get into safety?"

The answer isn't straightforward. In fact, it is doubly difficult to plan a career in safety engineering, assurance, or consultancy as a solid background in the underlying technologies (such as software, architectures, or databases) and sector knowledge (eg. aviation, nuclear or rail), plus the right opportunities all have to be present

Safety is often a second career, taken on by engineers or consultants who have already got several years of experience doing other things. Also, there is the issue that not many safety staff are required for most jobs: often there is only one safety engineer on smaller projects; if that role is already taken, there is little chance of a junior gaining relevant experience.

With this situation in mind, we continue our series of articles where members of the SCSC Steering Group share their experiences of 'getting into safety'. Some of the routes taken are definitely not linear!

Please read and compare with your own 'safety story'. Of course, these experiences are based on events some time ago, and the situation has definitely improved as the industry has matured. For example, there are now courses (at post-graduate level) on safety-critical systems such as those at the University York, there are competency frameworks for safety roles, and the SCSC has its own "Safety Futures Initiative" programme with the aim of developing young and early-career staff so that they can take on full safety roles.

The messages that come out of these experiences however, are that sometimes you do just have to be in the right place at the right time, and with the right underlying characteristics. All safety roles require the ability to be able to assess risk, to understand some difficult technical arguments, to follow (and create) workable processes, rules and regulations, to know the standards and guidelines relevant to the job in hand, to be able to communicate well, work in a team with colleagues, and very importantly, to be assertive and take a strong position when needed.

James Inge



As I was lucky enough to join the Ministry of Defence (MOD) straight from school as a sponsored student, I left university with practical engineering experience from placements around the MOD, not just an MEng. My first proper job after the MOD's graduate scheme was as a project manager in a "cluster team", responsible for procuring and supporting a variety of electronic systems myself. It was a steep learning curve but a great opportunity to experience different aspects of engineering management. Our team had no safety manager, so I soon realised it also fell to me to put in place safety cases for my kit.

After this, I joined the Defence Procurement Agency's Acquisition Safety and Environmental Support Group in 2005, working on the DPA's safety policy and rolling out the then-new Acquisition Safety and Environmental Management System. At first I thought that now I had my promotion, I would soon move on, but then I got the bug for trying to improve our management systems and make it easier for everyone to do better safety engineering. I studied Safety Critical Systems Engineering at York, became involved in development of Defence Standard 00-56 and other MOD safety standards and policy, and started networking through conferences and the IET.

Since then, I have led the MOD Ship Safety Management Office, been the Senior Engineer in a land systems delivery team, acted as the safety governance lead for one of our air domain business units, and led the central safety and environmental protection team: providing policy, assurance and governance for Defence Equipment and Support, as well as developing training and guidance material. Outside MOD I've also taken turns chairing the IET's System Safety Engineering professional network and the Independent Safety Assurance Working Group. I now lead DE&S's Ships Domain Safety and Environmental Protection team, am a member of the SCSC Steering Group, and am working on IEC 63187, a draft international standard for safety in the defence sector.

"Groups like the SCSC have been invaluable to help me learn and build the networks that have helped me develop"

Through my career, I've found it vital to be able to bring in ideas from different parts of the MOD, the defence industry, and beyond. To deliver good safety management policy and standards, I've also needed the experience of trying to put them into practice in project roles. Groups like the SCSC have been invaluable to help me learn and build the networks that have helped me develop.

Louise Harney



I never expected to study at the University of Oxford, and certainly not anywhere as prestigious as Christ Church. As an ambitious sixth-former at Greenhead College in Huddersfield, I applied mostly to the American universities I had watched movies about, imagining my Legally Blonde-esque arrival at Caltech where I was privileged to be accepted. Most certainly prompted by my parents, our highly-respected Vice Principal left a note on our class noticeboard for all to see. I've kept that note somewhere. It was my acceptance letter from Christ Church with his handwriting on the top right-hand corner "*This is where you should be.*" And he was right.

It seemed the whole college started asking me what I was going to do! That Vice Principal had taken us to all our debating competitions, supporting us to speak our minds and weigh up difficult options in public. People always talk about STEM like there is some magical moment that children and teenagers are inspired for their future lives and careers in tech, but I don't think that's true. There is an accumulation of support and self-belief that builds a way of thinking, from a number of sources – parents, wider family, teachers, friends, extra-curricular activities. Those formative debates, classes on interview technique and power of thought taught me the foundations of behavioural competency needed to work in the field of system safety, alongside the life lessons I already had from my family.

After three years of 'tutes' (tutorials) that required me to present my arguments to a small group; a lot of hard graft and incredible memories later, I started applying to jobs. Like many of my peers graduating with a degree in Physics, I naturally applied for the big corporate world of banking. I got lost in so many of those offices and felt nothing but out of place.

A friend at university advised me to think about consultancy – I was forever meddling in different societies and suggesting better ways of working – maybe that would suit me better. I'd never considered starting out as a consultant, I just assumed you had to already know a lot of stuff to be able to do that. Then I interviewed at a small consultancy, Helios, where (if I was successful) I would be the only graduate that year. It felt like a good fit straight away: the people were great; they worked hard to make me feel comfortable in the office and interview – and this office I couldn't get lost in, people even had keys to the front door!

The work sounded exciting, with many different challenges and the opportunity to see how different organisations do things. I was thrilled to be offered the job and for the next few years worked really hard, while travelling the world and making new friends. Helios happened to have a lot of safety work at the time, so I was lucky enough to go on a Eurocontrol course about developing safety cases. I was already hooked. Every catch up with my line manager, every annual appraisal, I would be asked if I wanted to expand my knowledge to other areas, airport performance maybe or noise management. Of course, I would be happy to do that if I needed to, and did dabble a little with other topics alongside my safety work, but nothing else chimed with me like developing a new safety management system or building a safety argument.

"Nothing else chimed with me like developing a new safety management system or building a safety argument"

I spent a lot of time working on radar upgrades and air traffic control. I had the rare opportunity to see all aspects of how an organisation worked, how they got their product or service through its entire lifecycle from concept to decommissioning, and to talk to so many different people across the globe. Facilitating workshops was my favourite thing to do, especially internationally. I was mentored by colleagues both internally and externally, with one-to-one support available all of the time. Knowledge and competency are something that has to be built and evolves your mindset as well as your technical skills, so no matter how many training courses you go on, support and supervision by an expert (that I was lucky enough to have so readily available) are essential to growing in your career. I can't thank those people enough for the support I received.

I loved the variety of working in a consultancy like this, being able to work with different organisations and deliver something really tangible every day, but I wondered what life would be like in industry and longed to see the actual product or service being designed in depth, so I made a leap into industry with Raytheon and later moved on to Leonardo, working on sensing technologies. I worked with complex systems; challenging international collaborations; and improving safety management systems.

I first came across the SCSC at Raytheon when my then-line manager invited me along to an event. I began to build a network of incredibly talented and helpful people, all working in the field I feel most at home in. I learned a huge amount technically, but I also made some great friends who I would continue to collaborate and socialise with as the years went by and we all moved between various day jobs. The consistency of the SCSC as a network; with working groups, conferences and much more; gave me the confidence to develop into a fully-fledged system safety engineer, now training, coaching and advising others on the subject alongside more technical development work. When I was invited to join the SCSC Steering Group, I felt I had 'made it'! I'm learning every day and the support available in the SCSC helps us all to do that, alongside more formal mentoring and support available in our day-to-day jobs.

"The consistency of the SCSC as a network; with working groups, conferences and much more; gave me the confidence to develop into a fully-fledged system safety engineer"

I have progressed through my career so fast, and looking back I have been incredibly lucky and grateful to be supported by a number of great line managers and mentors, while putting myself forward to take on interesting and challenging roles. If you don't ask, you don't get – I intend to keep asking for those exciting opportunities and to offer the same to those I work with. But safety isn't just a day job. It permeates all aspects of our lives, and that's what I love about it. Whether I'm working on the next generation of radar systems; sailing; or just trying to stop my son falling off yet another thing he has climbed on, there are risks. Risks are a necessary part of living, but with some clever engineering we can reduce those risks enough to keep taking them day after day.

Image attribution: top image 54463913 © Somsak Dalad | Dreamstime.com

National Space Centre Tech Trip Report

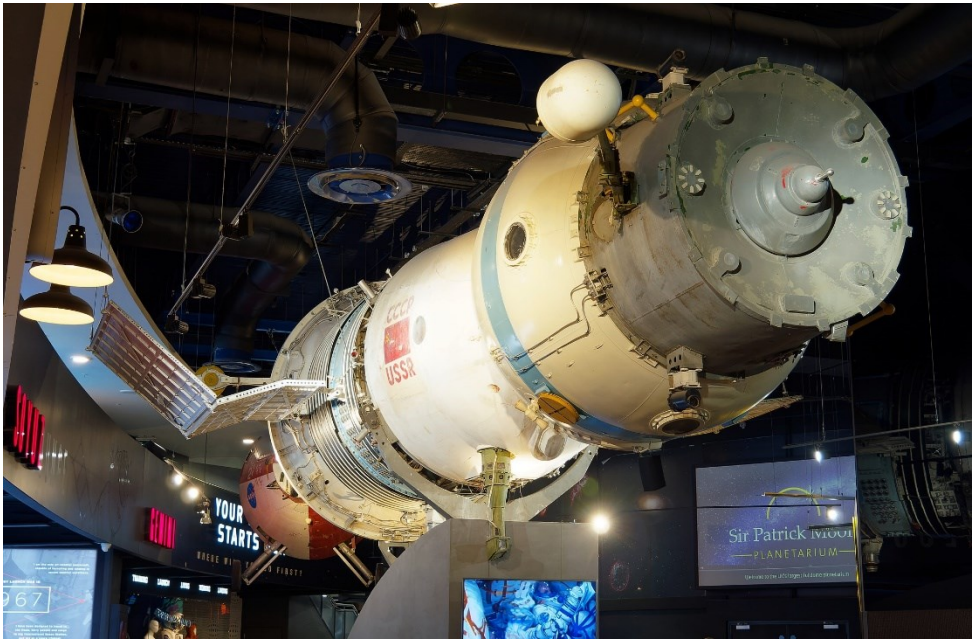


The SCSC's recent TechTrip was to the National Space Centre[2], Leicester on 24th June 2023. The trip, which was open to everyone, included a fabulous show in the UK's largest planetarium. Mike Parsons provides a report.

The space centre is about a mile from Leicester city centre, and can be accessed via a walk through a pleasant park. It is quite visible with an unusual inflated structure housing the rockets and is visible from a long way off.

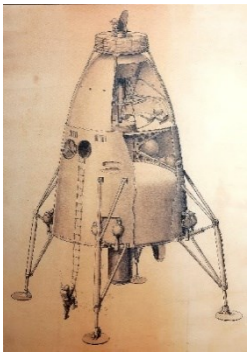
[2] https://www.spacecentre.co.uk/

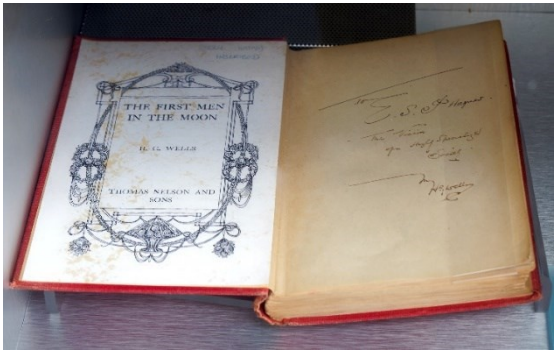
On entry we were greeted by an ancient Soyuz capsule.



We met up with the rest of the group, had a bite to eat, then proceeded to go up the tower that houses the two main rocket sections. At each level on the way up there were interesting exhibits, with lots from the early days of British rocket development. It was explained how we managed to launch a satellite from a cancelled programme and then feed the technology into European launcher developments. The satellite is still in orbit!

As well as the space hardware, there were early illustrations from the British Interplanetary Society





and an author-signed copy of H.G. Wells book 'The First Men in The Moon'

I thought the exhibits were well placed into their historic time context with the use of extensive timelines. These really helped to jog memories:



There was even a late sixties / early seventies living room on the top floor showing the sort of surroundings in which we all viewed the moon landings (I remember these colours well!)



On the ground floor were more exhibits including a mock-up of the Columbus module from the International Space Station:



We had an hour to spare before our booked show at the planetarium, so nipped out of the Space Centre and into the Abbey Pumping Station museum which is next door. The main attraction here is the pump room itself with massive Victorian beam engines. The columns, pistons and pumps were beautifully decorated, and it is interesting to compare and contrast with the Space technology next door:



We had a quick tour round the (closed) upper floors of the pump room by a very helpful member of the museum staff, before returning to the space centre for our planetarium show.

On entering the planetarium, we were bowled over by its size. The whole experience was amazing and our narrator for the show was very professional. The opening projection is very clever and makes you think you are entering an old observatory:



But this was soon replaced by a fantastic set of planet, stars and constellations:



It was an interesting visit and one recommended to space enthusiasts, especially those into early British space history. The pumping station next door is definitely worth adding to the trip, especially as it is free entry!

Leading image: Matt Brown, CC BY 2.0, all other photographs copyright of Mike Parsons.

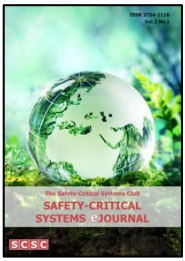


SSS 24 Posters

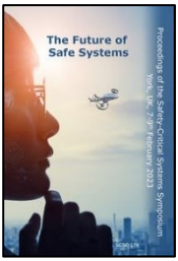
If you would like to present a poster at SSS'24 please contact mike.parsons@scsc.uk.

A poster is an opportunity to present your work in an informal way. There will be 2 dedicated poster sessions at the event and any associated abstracts or papers can be published in the symposium proceedings book. See https://scsc.uk/e1007 for more details.

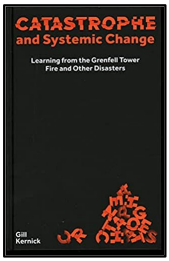
Recent Safety Publications



Safety-Critical Systems eJournal vol.2 no.2
Summer Issue 2023
scsc.uk/scsc-186



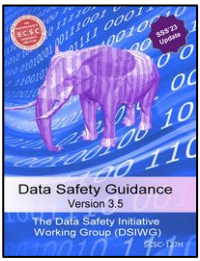
Proceedings of the 31st Safety-Critical Systems Symposium.
scsc.uk/scsc-179



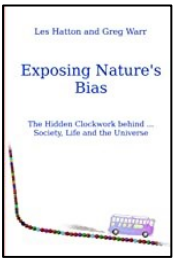
Catastrophe and Systemic Change. Learning from the Grenfell Tower Fire and Other Disasters.
https://www.amazon.co.uk/dp/1913019292



Guidance on the Safety Assurance of autonomous systems in Complex Environments.
http://www.york.ac.uk/assuring-autonomy/guidance/sace/



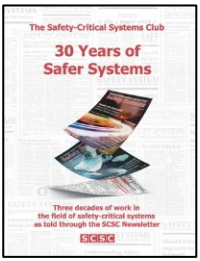
Guidance on the management of data safety risks (V3.5)
scsc.uk/scsc-127H



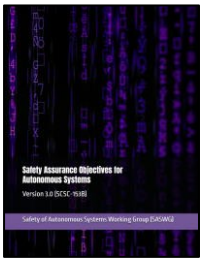
Revealing a newly discovered fundamental law of inequality.
http://www.amazon.co.uk/dp/1908422041



Guidance on assuring safety-related service (V3.1)
scsc.uk/scsc-156C

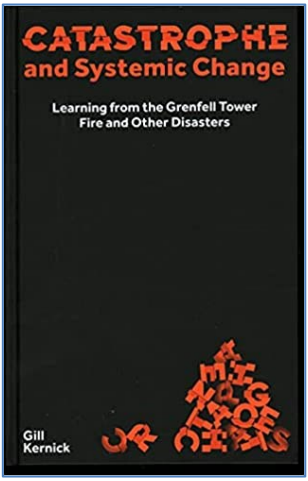


Three decades of work in the field of safety-critical systems as told through the SCSC Newsletter.
scsc.uk/scsc-169



Guidance on assuring autonomous systems.
scsc.uk/scsc-153B

Book Review



Somnath Pal reviews Gill Kernick's book "Catastrophe and Systemic Change". In the book, Gill gives a moving account of how she witnessed first-hand the Grenfell Tower fire of 2017. At the time of the fire, she was living in an adjacent block and having previously lived on the 21st floor in Grenfell Tower, she knew several people, some children, who died that night.

In response to the fire, Gill was committed to ensuring an event of this nature never happened again. She thought the desire to improve would be shared, but found this to be far from the case, and this led her to ask why this failure to learn makes sense and motivated her to write this book: "the book she wished she'd never had to write".

This book is essential reading, not only for those with management responsibility for high rise buildings, but also for anybody trying to understand why we still have events of this magnitude, such as Deepwater Horizon and the Boeing 737 MAX incidents.

I very much appreciate the writer's contemplation about why we do not learn and how instead of pointing at those responsible for the mismanagement of safety requirements, systemic change could be enabled. Her meticulous analysis of situations prior, during and after the catastrophic fire incident in Grenfell Tower, is elaborate and without bias. Particularly, highlighting the corporate marketing scandal in the tower refurbishment ignoring fire safety regulations, the shortfall in planning and decision making by Fire Brigade and loopholes in proper inspection by government authorities, are *to the point* and *crisply presented*.

The main agenda – being hopeful, that the readers ponder, question, logically debate and act upon the root cause – would definitely help prevent catastrophes of this scale and is really commendable. Gill's understanding, that the `system is perfectly designed to ensure that we do not learn`, is *noteworthy!*

Categorizing the analysis into Foundational, Behavioural, Relational and Contextual elements through Chapters 4 to 7, helps understand the magnitude and impact, viewed from different perspectives. Finally, Democratization of Change in Chapter 8, highlights the importance of the Process(es) followed to prevent future catastrophes. The book is enriched through 21 pictures and exhaustive 31 pages long list of references, which would help serious research on the unfortunate incident.

Gill also makes a crucial observation, that there is no incentive to *admit mistakes or learn from them*. Instead of preserving the status quo, avoiding taking ownership or responsibility of the cause and the consequence, she strongly suggested that all the stakeholders should work together through open exchange of expert views, to find the best option to mitigate hazard causes. She also distinctly identifies that *distributed decision making* by adaptive leadership through complex problem solving, critical thinking ability, creativity, emotional intelligence and cognitive flexibility are paramount to the leadership skills necessary for reducing the chances of occurrences of catastrophes.

Gill rightly points out that regulations are important inputs, but cannot guarantee safety. Secrecy, lack of accountability and inadequate competency are also equally responsible for obstructing the learning process. It is also imperative that the boundaries between the policy makers and the beneficiaries of the policy, be made seamless. She kept reminding us, that to save human lives and social structures, the risks with "*low probability and high consequences*", must be thoroughly investigated and mitigated (considering factors beyond cost alone).

I work within the domains of Safety and Reliability, and reading the book has motivated me in initiating discussions with the residents of my apartment community, about contacting Real Estate developers, Contractors, Fire Brigade, Police and Municipality to upgrade the preventive measures of handling Catastrophes caused by Fire.

I thank Gill for drawing our attention to a very important topic, while keeping the narrative engaging and the reader interested. This book does leave a lasting impression, forcing one to reflect on one's social, ethical and moral responsibilities. I wholeheartedly recommend this book, not only for reading, but also for propagating the fundamental ideas discussed.

Somnath Pal FIRSE, SMIEE

Chair, IEEE Reliability Society Hyderabad. Member, Safety Culture Working Group, UK.

Somnath Pal retired from Indian Railways after 37 years' experience in field maintenance of railway telecommunication equipment, microwave repairing laboratory and faculty in Central Signalling & Telecom Institute. He has presented several papers in International Railway Safety Council Conferences drawing from interactions with scholars and experts through association with IEEE and has a particular interest in accident investigation cases.

60 Seconds with ... Prof. Davy Pissoort



Davy Pissoort received his PhD degree in electrical engineering from Ghent University, Belgium in 2005. He then worked as an R&D Engineer at Agilent Technologies (now Keysight Technologies) in Ghent, Belgium. Since 2009, he has been a Professor at KU Leuven Bruges Campus, where he is one of the key founders of the Mechatronics Group.

His current research interests include EMI Risk Management as well as safety assurance of interconnected autonomous systems. Davy has also recently joined the SCSC Steering Group.

What first attracted you to working in the field of System Safety?

I was initially drawn to the field of System Safety through my work in electromagnetic compatibility (EMC). While working in EMC, I became involved in various working groups focused on the connection between EMC and functional safety, led by Keith Armstrong. As I delved deeper into the world of functional safety, I found myself increasingly intrigued by its complexities and significance.

Keith also played a pivotal role in guiding my journey when he introduced me to the Safety-Critical Systems Club and, more notably, the Safety-Critical System Symposium. These experiences opened my eyes to a broader community of experts and innovative ideas in the field of System Safety.

My fascination with System Safety was further fuelled by the evolution towards autonomous systems, an area that greatly piqued my interest. The intersection of EMC, functional safety, and the exciting advancements in autonomous technology all came together to solidify my passion for working in the field of System Safety.

What aspect of your career are you most proud of?

Related to System Safety, I'm specifically proud of two things in my career. Firstly, I've secured funding for several EU-funded Marie-Curie Doctoral Networks. Two of these projects (SAS and PETER) focus on making autonomous systems safer and managing the risk of electromagnetic interference. Through these projects, not only has my own research team grown, but we've also nurtured a talented group of PhD researchers across Europe who are working on these important topics.

Secondly, one of my greatest sources of pride is when a PhD student I've mentored successfully graduates. It's amazing to watch them develop and learn over the years, and knowing that I've played a part in their growth is truly fulfilling.

Tell us one interesting unusual fact about yourself!

Sure, here's a fun fact about me: in addition to my Master's and PhD degrees in engineering, I'm also a certified soccer coach for really young kids, specifically those aged 6-7 years old. So, alongside all the technical stuff, I have this official qualification that lets me teach and train little soccer stars in the making!

What advice would you give to yourself age 12?

If I could talk to my 12-year-old self, I'd say, "Believe in yourself more!" Self-confidence will help you achieve amazing things in the future. Don't doubt yourself – you're capable of more than you can imagine.

What future changes would you like to see in the field of System Safety?

I hope people will increasingly look beyond just following the rules and standards. Sometimes, we get too caught up in ticking boxes, especially in my area of EMC. This can be counterproductive when it comes to safety-critical systems.

One exciting direction is how we can use Artificial Intelligence (AI) and Machine Learning (ML) to enhance system safety. It's a complex journey, but we're taking small steps. For instance, one of my PhD students, Laure Buysse, is exploring how we can monitor and analyse all the assumptions in our safety case during operation using AI/ML. The ultimate goal is to use this data to improve safety significantly.

What's your most favourite quote or motto?

"*Be who you needed when you were younger*". Something that I regularly keep in mind when supervising my PhD student**.**

If you could learn to do anything, what would it be?

If I could pick up a new skill, I'd choose to master "double-unders." It's something I've been working on for quite a few years, especially because I'm into CrossFit. Double-unders are a challenging jump rope technique where the rope passes under your feet twice with each jump. It's a skill that requires precision and coordination, and I'd love to conquer it.

If you could be any fictional character, who would you choose?

If I could step into the shoes of any fictional character, I think I'd choose to be Sherlock Holmes. His brilliant mind, deductive reasoning, and knack for solving mysteries have always fascinated me.

Artificial Intelligence - a positive revolution or are we all doomed!?

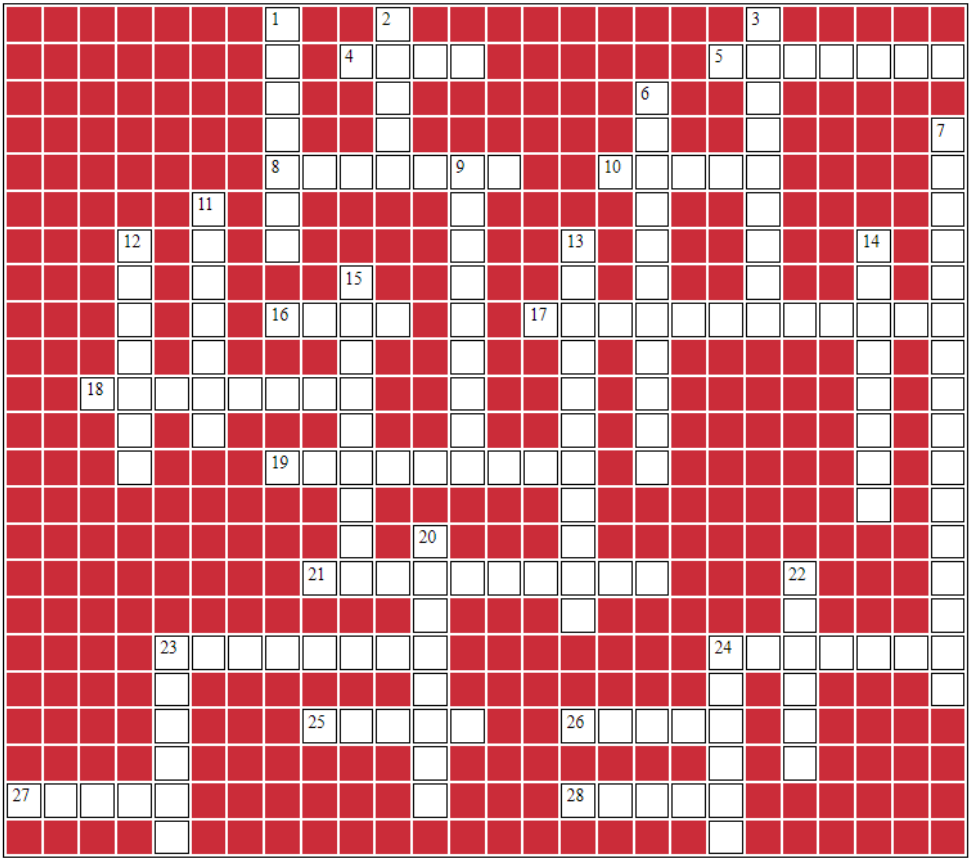
I believe that AI is primarily a positive evolution. AI has the potential to bring about many beneficial changes in our lives. However, we must handle it with care and responsibility as humans. System Safety plays a crucial role in ensuring AI is safe and trustworthy. Interestingly, AI itself can contribute to improving safety, which makes it a valuable tool for our future. So, it's not a question of being doomed but rather about using AI wisely for our benefit.

Safety Systems Crossword

Welcome to the 2nd Safety Systems Crossword prize competition where you can test your knowledge of the world of System Safety!

Send you completed grids to crossword@scsc.uk or hand them in at SSS'24 by 14th Feb 2024.

The first correct answer drawn from a hat at SSS'24 will win a £50 Amazon Voucher!



Across

4. Contemporary programming language emphasising performance, type safety, memory safety and concurrency (4)
5. Name of a Swedish mathematician that gave his name to a reliability distribution (7)
8. Chatbot developed by openAI and launched Nov 2022 (7)
10. Google subsidiary providing driverless cars in San Francisco (5)
16. University city, home to the Institute of Autonomy (4)
17. A word used to refer to the information and entertainment screens of a car (12)
18. Surname of woman credited with inventing the term "software engineering" (8)
19. Relating to knowledge or to the degree of its validation (9)
21. Airspace allocated for exclusive use by specific users like drones (10)
23. Evidence for a goal in Goal Structuring Notation (8)
24. Event that led to the largest single rail disaster in world history (7)
25. Logic symbols in fault tree diagrams (5)
26. Largely preventable event seriously affecting patient safety that should not occur (5)
27. Safety device used by mariners to signal for help (5)
28. Submersible that imploded when visiting the Titanic (5)

Down

1. Abbreviation for the European Organisation for Civil Aviation Equipment (7)
2. The basic unit of information in quantum computing (5)
3. Name of the numerical sequence calculated by the first ever computer program (9)
6. Device that produces a response when it receives a radio-frequency interrogation (11)
7. An algorithm exhibiting different behaviours on different runs, even with same inputs (16)
9. Possible impact reduction system for a drone (9)
11. Programme intended to reestablish a human presence on the moon (7)
12. Detection technique that uses AI to identify abnormal behaviour (7)
13. The quality of being noticeable or easy to see (11)
14. Technique or process that involve randomness in its design (8)
15. Able to be broken up into fragments, eg. on impact (9)
20. 24-story tower block engulfed by fire in 2017 (8)
22. Type of network used for machine learning (6)
23. Spacecraft manufacturer, launch service provider and satellite comms company (6)
24. Test to demonstrate if machine behaviour is indistinguishable from human (6)

Connect

The Newsletter and eJournal

Do you have a topic you'd like to share with the systems safety community? Perhaps an interesting area of research or project work you've been involved in, some new developments you'd like to share, or perhaps you would simply like to express your views and opinions of current issues and events. There are now two publishing vehicles for content – shorter, more informal content, can be published in the Newsletter with longer, more technical peer-reviewed material more suitable for the eJournal. If you are interested in submitting content, then get in touch with Paul Hampton for Newsletter articles: paul.hampton@scsc.uk or John Spriggs for eJournal papers: john.spriggs@scsc.uk

The SCSC Website

Visit the Club's website thescsc.org for more details of the Safety-Critical Systems Club including past newsletters, details of how to get involved in working groups and joining information for the various forthcoming events.

Facebook

Follow the Safety-Critical Systems Club on its very own Facebook page.

www.facebook.com/SafetyClubUK

Twitter

Follow the Safety-Critical Systems Club's Twitter feed for brief updates on the club and events: @SafetyClubUK

LinkedIn

You can find the club on LinkedIn. Search for the Safety-Critical Systems Club or use the following link:

www.linkedin.com/groups/3752227

Advertising

Do you have a product, service or event you would like to advertise in the Newsletter? The SCSC Newsletter can reach out to 1,000 of individuals involved in Systems Safety and so is the perfect medium for engaging with the community. For prices and further details, please get in touch with the Newsletter Editor.

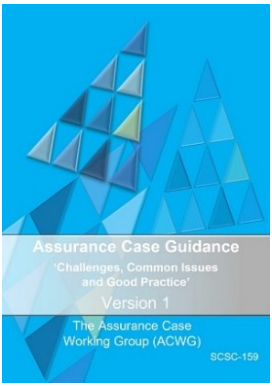
SCSC Working Groups

The Safety-Critical Systems Club is committed to supporting the activities of working groups for areas of special interest to club members. The purpose of these groups is to share industry best practice, establish suitable work and research programmes, develop industry guidance documents and influence the development of standards.

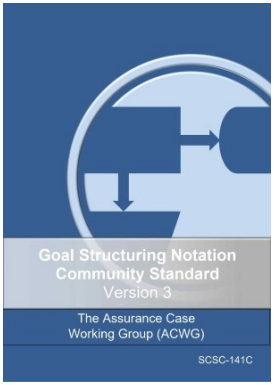
Assurance Cases

The Assurance Cases Working Group (ACWG) has been established to provide guidance on all aspects of assurance cases including construction, review and maintenance. The ACWG will:

- Be broader than safety, and will address interaction and conflict between related topics
- Address aspects such as proportionality, rationale behind the guidance, focus on risk, confidence and conformance
- Consider the role of the counter-argument and evidence and the treatment of potential bias in arguments



In Aug 2021, the group published v1.0 of the Assurance Case Guidance: scsc.uk/scsc-159



One of the working group's activities is the maintenance of the Goal Structuring Notation (GSN) Community standard.

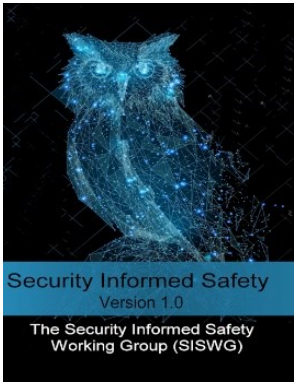
See scsc.uk/gsn for further details.

In May 2021, the group published v3.0 of the standard: scsc.uk/scsc-141C

Lead **Phil Williams** phil.williams@scsc.uk

SCSC Working Groups

Security Informed Safety



The Security Informed Safety Working Group (SISWG) aims to capture cross-domain best practice to help engineers find the 'wood through the trees' with all the different security standards, their implication and integration with safety design principles to aid the design and protection of secure safety-critical systems and systems with a safety implication.

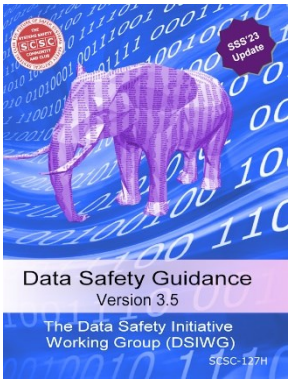
The working group aims to produce clear and current guidance on methods to design and protect safety-related and safety-critical systems in a way that reflects prevailing and emerging best practice.

The guidance will allow safety, security and other stakeholders to navigate the different security standards, understand their applicability and their integration with safety principles, and ultimately aid the design and protection of secure safety-related and safety-critical systems.

Lead **Stephen Bull** stephen.bull@scsc.uk

Data Safety Initiative

Data in safety-related systems is not sufficiently addressed in current safety management practices and standards.



It is acknowledged that data has been a contributing factor in several incidents and accidents to date, including events related to the handling of Covid-19 data. There are clear business and societal benefits, in terms of reduced harm, reduced commercial liabilities and improved business efficiencies, in investigating and addressing outstanding challenges related to safety of data.

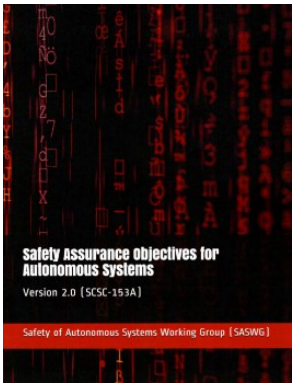
The Data Safety Initiative Working Group (DSIWG) aims to have clear guidance on how data (as distinct from the software and hardware) should be managed in a safety-related context, which will reflect emerging best practice.

An update to the guidance (v3.5) was published in Jan 2023: scsc.uk/scsc-127H

Lead **Mike Parsons** mike.parsons@scsc.uk

SCSC Working Groups

Safety of Autonomous Systems



The specific safety challenges of autonomous systems and the technologies that enable autonomy are not adequately addressed by current safety management practices and standards.

It is clear that autonomous systems can introduce many new paths to accidents, and that autonomous system technologies may not be practical to analyse adequately using accepted current practice. Whilst there are differences in detail, and standards, between domains many of the underlying challenges appear similar and it is likely that common approaches to core problems will prove possible.

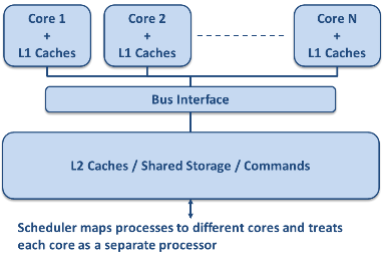
The Safety of Autonomous Systems Working Group (SASWG) aims to produce clear guidance on how autonomous systems and autonomy technologies should be managed in a safety-related context, in a way that reflects emerging best practice.

The group published v3 of its guidance Safety Assurance Objectives for Autonomous Systems, in Jan 2022 scsc.uk/scsc-153B

Lead Philippa Ryan pmrc@adelard.com

Multi- and Manycore Safety

It is becoming harder and harder to source single-core devices and there is a growing need for increased processing capability with a smaller physical footprint in all applications. Devices with multiple cores can perform many processes at once, meaning it is difficult to establish (with sufficient evidence) whether or not these processes can be relied upon for safety-related purposes.



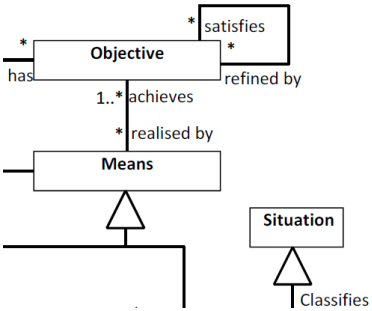
Parallel processes need to access the same shared resources, including memory, cache and external interfaces, so they may contend for the same resources. Resource contention is a source of interference which can prevent or disrupt completion of the processes, meaning it is difficult to know with a defined uncertainty the maximum time each process will take to complete (Worst Case Execution Time, WCET) or whether the data stored in shared memory has been altered by other processes.

The Multi- and Manycore Safety Working Group (MCWG) has been established to explore the future ways of assuring the safety of multi- and manycore implementations.

Lead Lee Jacques Lee.Jacques@leonardocompany.com

SCSC Working Groups

Ontology



The Ontology Working Group (OWG) develops ontologies that will form the basis of SCSC guidance, as well as having wider industrial and academic applications.

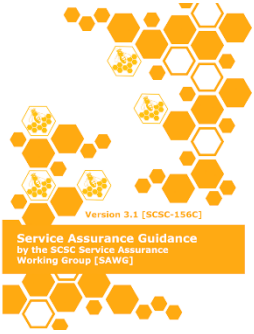
The OWG is currently working on the definition of an ontology of risk for application in guidance for risk-based decision making – notably safety and security – and for which ISO 31000 Risk Management principles are to be applied.

The Data Safety Working Group (DSIWG) developed the core aspects of the Risk Ontology, which has been migrated to this working group. The Risk Ontology will form the upper ontology to the Data Safety Ontology that the DSIWG will continue to develop.

Lead Dave Banham ontology@scsc.uk

Service Assurance

Risks presented by safety-related services are rarely explicitly recognised or addressed in current safety management practices, guidelines and standards. It is likely that service (as distinct from system) failures have led to safety incidents and accidents, but this has not always been recognised. The Service Assurance Working Group (SAWG) has been set up to produce clear and practical guidance on how services should be managed in a safety-related context, to reflect emerging best practice.

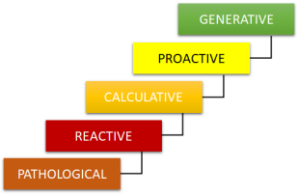


The group published v3.1 of the guidance in Jan 2023: scsc.uk/scsc-156C

Lead Kevin King kevin.king@baesystems.co.uk

SCSC Working Groups

SCSC Safety Culture



The Safety Culture Working Group (SCWG) has been established to provide guidance on creating and maintaining an effective safety culture. The group seeks to improve safety culture in safety-critical organisations focussed on product and functional safety, by sharing examples and latest approaches collated from real-life case studies.

Meetings provide an opportunity to discuss any particular aspects attendees are interested in taking forward, and to help set future directions for the group.

Lead **Michael Wright** michael.wright@greenstreet.co.uk

Systems Approach to Safety of the Environment



The Systems Approach to Safety of the Environment Working Group (SASEWG) is a new group intending to apply Systems Safety practices to systems that are embedded within the natural environment, while focussing on that environment.

The group aims to produce clear guidance on how engineered systems should be developed and managed throughout their entire lifecycle so as to preserve, protect and enhance the environment.

Since holding its inaugural meeting on 17th June 2022 the group is now well underway with its last meeting held on 9th July 2023. Please get in touch with the working group lead if you would like to join or find out more about this group.

Lead **James Inge** james.inge@scsc.uk

Safer Complex Systems



The Safer Complex Systems Working Group (SCSWG) builds on the IET/RAE work already done in this area. It is recognised that the RAE work is ongoing and collaboration is encouraged. The group's mission is to produce practical guidance on developing, managing and assuring complex systems throughout their lifecycle (so as to achieve and justify their safety).

The fourth meeting of the SCSC Safer Complex Systems Working Group took place on 14th September 2023 with the next meeting planned for 19th October 2023. Contact the group lead if you would like to attend or find out more about the working group.

Acting Lead **Mike Parsons** mike.parsons@scsc.uk

SCSC Membership

The SCSC provides a range of services to the System Safety community including seminars, tutorials, leadership events, specialist topic working groups, the annual symposium and a comprehensive body of publications. Membership brings many valuable benefits such as free access to online events, the SCSC Newsletter and access to presentations and other resources from events.

Individual Membership

To become an individual member of the SCSC please register on the SCSC website using the icon at the top right of any page and select "Register". Complete and save your account registration and then verify your email address. Once registered and logged in click the link "why not join the SCSC..." inviting you to become a member at the top right of the page or select "Pay membership" from the icon.

Individual membership can be paid online using a credit/debit card through our secure payment partner Realex Global Payments or contact Alex King for other payment methods. For student or retired member rates please contact Alex King to get your account status changed.

Corporate Membership

Your company contact with the SCSC should arrange the membership and any renewals for your organisation. To join as a member covered by a corporate membership, register as per the instructions for an individual member and then contact Alex King to confirm your affiliation.

Renewing Membership

You should be notified by email when your membership is almost expired or shortly after it has expired. These notifications will contain a link to the online renewal page or you will be able to renew when logging onto the website through the 'click to renew' link.

Membership Fees

The following fees are applicable for new and renewing members:

- 1 year Individual Membership: £140
- 2 year Membership: 11% discount: £250
- 3 year Membership: 17% discount: £350 (3 years for the price of 2)
- 1 year SFI Membership: FREE for first year, £35 for years 2 & 3
- 1 year Membership, retired member rate: £35
- For Corporate Membership discounts contact Alex King.

A one-month Publication Pass is also available for £15. This allows access to all SCSC website publications in a particular calendar month.

Contact Alex King using office@scsc.uk

The SCSC Steering Group


Tom Anderson
Honorary member


Stephen Bull
stephen.bull@scsc.uk


Dai Davis
Honorary member


Zoe Garstang
zoe.garstang@scsc.uk


Louise Harney
louise.harney@scsc.uk


Brian Jepson
brian.jepson@scsc.uk


Graham Jolliffe
Honorary member


Alex King
alex.king@scsc.uk


Wendy Owen
wendy.owen@scsc.uk


Davy Pissoort
davy.pissoort@scsc.uk


Roger Rivett
roger.rivett@scsc.uk


Emma Taylor
Honorary member


Sean White
sean.white@scsc.uk


Robin Bloomfield
Honorary member


Dewi Daniels
dewi.daniels@scsc.uk


Jane Fenn
jane.fenn@scsc.uk


Paul Hampton
paul.hampton@scsc.uk


James Inge
james.inge@scsc.uk


Nikita Johnson
nikita.johnson@scsc.uk


Tim Kelly
Honorary member


Mark Nicholson
mark.nicholson@scsc.uk


Mike Parsons
mike.parsons@scsc.uk


Felix Redmill
Honorary member


John Spriggs
john.spriggs@scsc.uk


Phil Williams
Honorary member

Club Positions

The current and previous (marked in italics) holders of club positions are as follows:

Managing Director

Mike Parsons 2019-

Tim Kelly 2016-2019

Tom Anderson 1991-2016

Programme & Events Coordinator

Mike Parsons 2014-

Chris Dale 2008-2014

Felix Redmill 1991-2008

Newsletter Editor

Paul Hampton 2019-

Katrina Attwood 2016-2019

Felix Redmill 1991-2016

eJournal Editor

John Spriggs 2021-

Diversity, Equity and Inclusion (DE&I) Lead

Wendy Owen 2023-

Steering Group Chair

Roger Rivett 2019-

Graham Jolliffe 2014-2019

Brian Jepson 2007-2014

Bob Malcolm 1991-2007

Manager

Alex King 2019-

Honorary Solicitor

Dai Davis 2022-

University of York Coordinator

Mark Nicholson 2019-

Website Editor

Brian Jepson 2004-

Administrator

Alex King 2016-

Joan Atkinson 1991-2016

Safety Futures Initiative Leads

Zoe Garstang 2019-
Nikita Johnson 2023-

Nikita Johnson 2019-2021

Calendar

October '23

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

November '23

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

December '23

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

January '24

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February '24

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29			

March '24

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

April '24

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

May '24

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

June '24

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

July '24

M	T	W	T	F	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

August '24

M	T	W	T	F	S	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

September '24

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Events Diary



10-12 Oct 2023
Conference

RSSRail 2023: International conference on reliability, safety and security of railway systems

Berlin, Germany

rssr2023.ebuef.de

16 Oct 2023
SCSC Working Group

SISWG: SISWG Guidance Development

Online

scsc.uk/e1075

17 Oct 2023
Conference

HISC 2023: High Integrity Software Conference

Bristol, UK

www.his-conference.co.uk

19 Oct 2023
SCSC Working Group

SCSWG#5 SCSC Safer Complex Systems Working Group meeting #5

Online

scsc.uk/e1069

20 Oct 2023
SCSC Working Group

SAWG#80: SCSC Data Safety Initiative Working Group meeting #80

Online

scsc.uk/e1069

1-2 November 2023
Conference

IET SCS: Safety Critical Systems training course: Managing systems, hardware and software safely

Online

safetysystems.theiet.org

9 Nov 2023
SCSC Working Group

SCSC-OWG: Risk Ontology Meeting #79

Online

scsc.uk/e1077

13-15 Feb 2024
SCSC Symposium

Safety Critical Systems Symposium SSS'24

Bristol, UK

scsc.uk/e1007

Partner Event



The High Integrity Software Conference #HISConf2023

www.his-conference.co.uk

The mission of the High Integrity Software Conference (HISC) is to share challenges, best practice and experience between software engineering practitioners. The conference features talks from industrial and academic specialists, which disseminate experience and knowledge of important techniques and methods that are applicable across industry sectors.

This year marks the 10th anniversary of HISC, and for the first time proposals have been invited for talks via a CfP (Call-for-Presentations) system, further information available in the Call for Presentations tab on the website.

Registration for HISC 2023 is open and there are a limited number of delegate tickets available so don't hesitate and register today!

To see the full programme and book your place - https://www.his-conference.co.uk/

All delegate tickets are £264.00 (inc. VAT) per person.

If you have any questions about the conference, the exhibitor package or further sponsorship opportunities, contact info@his-conference.co.uk.


SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY
SSS'24
32nd Safety-Critical Systems Symposium
13-15th February 2024
Bristol Royal Marriott Hotel, UK